Центр правовой трансформации
А.Пазюк, М.Соколова

УЧЕБНОЕ ПОСОБИЕ

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: ВВЕДЕНИЕ В ПРОБЛЕМАТИКУ

Минск 2015

LAWTREND
исследования образование действия

УЧЕБНОЕ ПОСОБИЕ

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: ВВЕДЕНИЕ В ПРОБЛЕМАТИКУ

Пазюк А., Соколова М.
Защита персональных данных: введение в проблематику: учебное пособие / А. Пазюк, М.Соколова. – Минск, 2015. – 116 с.

Авторы учебного пособия, основная цель которого - введение в общий контекст защиты персональных данных как проблемы публичной политики, основное внимание уделяют рассмотрению различных трактовок понятия «персональные данные», анализу целей защиты персональных данных в контексте социально-этической проблематики, выявлению структурных элементов защиты персональных данных, характеристике стратегий и форм правового регулирования обращения персональных данных и защиты соответствующих прав человека и др. Учебное пособие предназначено для всех, кто интересуется проблемой сохранения и защиты приватности в цифровом мире.

ISBN

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

Учебное пособие «Защита персональных данных: введение в проблематику» предназначено для всех, кто интересуется проблемой сохранения и защиты приватности в цифровом мире.

Цель пособия – введение в общий контекст защиты персональных данных как проблемы публичной политики. Основное внимание поэтому уделяется рассмотрению различных трактовок понятия «персональные данные»; анализу целей защиты персональных данных в контексте социально-этической проблематики; выявлению структурных элементов защиты персональных данных; характеристике стратегий и форм правового регулирования обращения персональных данных и защиты соответствующих прав человека; подходам к методике анализа национальных режимов защиты персональных данных.

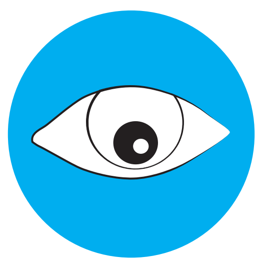
Пособие состоит из трех разделов. В первом, вводном, разделе «Неприкосновенность частной жизни и защита персональных данных» представлена характеристика соответствующей терминологии, анализируются основные угрозы приватности в цифровую эпоху. Во втором разделе «Защита персональных данных как проблема публичной политики» предлагается вариант структурирования проблемы на основании содержания (обеспечение качества обработки данных и гарантий прав субъектов данных), акторов и набора инструментов регулирования политики в отношении защиты персональных данных. Третий раздел «Правовые аспекты защиты персональных данных» включает подразделы «Международные принципы и стандарты», «Национальные режимы правового регулирования». В заключительном разделе «Итоговый практикум» дана схема для сравнительного анализа законодательства в сфере защиты персональных данных.

Концептуальную основу пособия составляют теоретические подходы, предложенные А. Уэстином, Ч. Раабом, К. Беннетом, Л. Байгрэйвом и К. Гринлифом[1]. В рамках этих подходов эффективный режим политики в отношении персональных данных определяется как использование комплекса разнообразных инструментов регулирования и вовлечение различных акторов в процессы структурирования проблемы защиты персональных данных и принятия решений в этой сфере.

1 Westin, A. (2003) Social and Political Dimensions of Privacy. Доступно через: http://www.asc.upenn.edu/usr/ogandy/Gandy%20Comm664/westin%20-%20social%20and%20political%20dimensions%20of%20privacy.pdf; Bennett, C. (2001) What Government Should Know about Privacy: A Foundation Paper. Доступно через: http://www.colinbennett.ca/wp-content/uploads/2012/06/What-Government-Should-Know-about-Privacy.pdf; Bennett, C. (2008) The Privacy Advocates: Resisting the Spread of Surveillance. Cambridge, MA: MIT Press; Bennett, C. Grant, R. (1999) Visions of Privacy: Policy Choices for the Digital Age. Toronto: University of Toronto Press; Bennett, C. and Raab, C. (2006) The Governance of Privacy: Policy Instruments in Global Perspective. Cambridge, MA: The MIT Press; Bygrave, L. (2002) Data Protection Law: Approaching its Rationale, Logic and Limits. The Hague: Kluwer Law International; Greenleaf, G. (2011) Global Data Privacy in a Networked World. Доступно через: http://ssrn.com/abstract=1954296

Раздел 1.

НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ





ХАРАКТЕРИСТИКА ОСНОВНЫХ ПОНЯТИЙ

ЧАСТНАЯ ЖИЗНЬ

Хотя общепринятой трактовки понятия «частная жизнь» не существует, большинство теоретиков сходятся в том, что термином «частная жизнь» обозначаются

- *сферы жизни человека, которые он не желает делать достоянием других (физических и юридических лиц, органов и должностных лиц государственной власти);*
- *«личное усмотрение» - свобода от внешнего управляющего воздействия и контроля государства, общественных организаций, граждан в рамках этих сфер и возможность контролировать их*[1].

Понятие «частная жизнь» включает два аспекта: (1) сферы жизни человека, которые он не желает делать достоянием других; (2) свобода от внешнего управляющего воздействия и контроля в рамках этих сфер.

Информационная составляющая частной жизни включает:

- *любого рода фактические данные о событиях, связанных с телом человека: факты о болезни лица, составляющие медицинскую тайну; сведения о терапевтическом или хирургическом лечении; фактические данные о смерти и о судьбе человеческих останков;*
- *фактические сведения, затрагивающие семейную жизнь: персональные данные, кроме общедоступных данных гражданского состояния; о фактах рождения; о фактах заключенных браков; о фактах смертей; о секрете материнства и о секрете усыновления;*
- *сведения о фактах сексуальной жизни и о чувствах лица; о фактах существования любовных отношений вне семьи или о факте их разрыва;*
- *сведения о внутренних убеждениях индивида: политические и философские взгляды*[2]

Выведенная на «орбиту» прав человека частная жизнь обретает статус права на частную жизнь, которое «позволяет человеку чувствовать себя человеком»[3]. Хотя категория «частная жизнь» не имеет нормативного (прописанного в документах) юридического содержания, правовое регулирование устанавливает пределы ее не-

1 Шахов Н. (2008) Отношения по охране частной жизни и информации о частной жизни как объект теоретико-правового исследования. Ростов-на Дону. С. 7

2 Bernard A. La protection de l'intimité par la droit privé: eloge du ragot ou comment vices exposes engendrent vertu. Les For Interieur, p.153-179. Доступно через http://www.u-picardie.fr/labo/curapp/revues/root/35/alain_bernard.pdf_4a081e8ad4544/alain_bernard.pdf Цит по Ариков, Г. (2014) Аспекты неприкосновенности частной жизни в уголовном законодательстве Республики Молдова

3 Bygrave L.A. Privacy and Data Protection in an International Perspective. In: Stockholm Institute for Scandinavian Law & Lee A Bygrave 2010. p.165-200 Доступно через: http://www.uio.no/studier/emner/jus/jus/JUS5630/v13/undervisningsmateriale/privacy-and-data-protection-in-international-perspective.pdf (date of visit: 19.02.2013); Назаров, Б.Л. (1995) Права человека История, теория и практика: Учебное пособие – Москва:.: Русспит

прикосновенности (приватность, privacy) и, следовательно, пределы допустимого вмешательства[1]. Благодаря практике правоприменения статьи 8 Европейской Конвенции о защите прав и основных свобод человека (1950 г.) это понятие приобрело четкую нормативную трактовку в заявлении Европейского суда по правам человека (1992 г.):

> *«Частная (личная) жизнь – это емкая категория, которой невозможно дать исчерпывающее определение. Каждый человек волен развивать это понятие и наполнять его определенным смыслом. Было бы непозволительно ограничить понятие [личной жизни] «внутренним кругом» … и исключить целиком внешний мир, не входящий в этот круг. Таким образом, понятие личной жизни с необходимостью включает право на развитие взаимоотношений с другими лицами и внешним миром»[2].*

Составляющими частной жизни, согласно прецедентному праву Европейского Суда по правам человека, являются:

- *персональная идентификация. Данный вопрос касается, прежде всего, изменения фамилии, регистрации имен, а также изменения пола и внесения соответствующих исправлений в акты гражданского состояния (Гийо против Франции (1993); В. против Франции (1992));*
- *определение законных связей. Важной составляющей частной жизни является доступ человека к информации о своем прошлом и своих родственных связях (Гаскин против Великобритании, 1983), возможность не только установления, но и оспаривания отцовства (Расмюссен против Дании, 1984);*
- *физическая и моральная неприкосновенность. Обязательные медицинские обследования, принуждение к медицинскому и психиатрическому лечению, физическое насилие и отсутствие юридической возможности привлечь виновных к ответственности (X & Y против Нидерландов, 1996[3]), запрет на добровольную смерть (Претти против Великобритании, 2002) и на аборт по медицинским показаниям (Тисяк против Польши, 2007) могут быть признаны вмешательством в частную жизнь;*
- *личное пространство. Речь идет об «экологических» правах человека, а также о публикации фотографий и информации личного характера (Фон Ганновер против Германии, 2004);*
- *сбор и использование информации. Современное общество невозможно представить без систем наблюдения, дактилоскопии, баз ДНК, официальной переписи населения – но ведь вся собранная таким образом информация, безусловно, касается частной жизни;*
- *доступ к персональным данным. Несмотря на то, что определенная информация может подлежать хранению, это не обязательно означает, что лицо, о котором она собрана, будет иметь автоматический доступ к ней (Леандэр против Швеции, 1987);*

1 Авдеев, М.Ю. (2013) Законодательство Российской Федерации о неприкосновенности частной жизни: к вопросу о заимствовании зарубежного опыта. Доступно через: http://cyberleninka.ru/article/n/zakonodatelstvo-rossiyskoy-federatsii-o-neprikosnovennosti-chastnoy-zhizni-k-voprosu-o-zaimstvovanii-zarubezhnogo-opyta

2 Красотенко, О.Ю. Понятие «частная жизнь» в решениях Европейского Суда по правам человека. Минск, 2011. Доступно через: http://elib.bsu.by/handle/123456789/29040

3 В деле X & Y против Нидерландов суд признал, ЧТО [Статья 8] не только принуждает государство воздерживаться от ... вмешательства: в дополнении к этому негативному первоначальному обязательству могут быть и положительные обязательства, неотъемлемые от действительного уважения личной и семейной жизни... Эти обязательства могут включать в себя принятие мер, направленных на обеспечение уважения личной жизни даже в сфере отношений между отдельными личностями.

- *сексуальные отношения. Сексуальная жизнь отдельного лица является частью и важным аспектом его личной жизни. Заявители в Европейском Суде отстаивали свое право на гомосексуальные отношения (Даджен против Великобритании), садомазохистские практики (Ласки, Джаггард и Браун против Великобритании) и публичную демонстрацию сексуального поведения;*
- *социальная активность. Возможность эффективного взаимодействия с другими людьми (МакФили против Великобритании (1980), Сливенко и др. против Латвии (2003));*
- *профессиональные взаимоотношения. По мнению Суда, нет принципиальных оснований полагать, что понятие «частной жизни» исключает деятельность профессионального и делового характера, именно в своей работе большинство людей имеют значительное, если не наибольшее, количество шансов развивать отношения с внешним миром (Нимиц против Германии. 1992)*[1].

ПРИВАТНОСТЬ, PRIVACY И НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ

Общим эквивалентом понятия «неприкосновенность частной жизни» и термина «privacy», используемого в международных документах, является заимствованное из латинского языка слово «приватность» в значениях свобода, интимность, секретность, одиночество, собственность, личность, межличностные отношения.

> *В данном курсе понятия приватность и неприкосновенность частной жизни рассматриваются как синонимичные. Термин «приватность» при этом представляется более предпочтительным, поскольку в меньшей мере акцентирует физические аспекты неприкосновенности личности.*

Общим эквивалентом понятия «неприкосновенность частной жизни» и термина «privacy», используемого в международных документах, является заимствованное из латинского языка слово «приватность» в значениях свобода, интимность, секретность, одиночество, собственность, личность, межличностные отношения.

Каждое из этих значений может быть конкретизировано:

- *«одиночество» - добровольность/вынужденность одиночества, полное/частичное одиночество, длительность одиночества и т.д., а также действий, ведущих к одиночеству или его отсутствию;*
- *свобода от вмешательства других;*
- *право на секретность информации о себе;*
- *в сфере собственности – «право на личную территорию»*[2].

Этимология понятия *«приватного»* связана с индоевропейским прилагательным *«priyos» - «(свой)* собственный», «милый, дорогой, любимый». Со временем *«priyos»* начинает служить наименованием группы общества, а затем и положения в обще-

1 Красотенко, О.Ю. Понятие «частная жизнь» в решениях Европейского Суда по правам человека. Минск, 2011. Доступно через: http://elib.bsu.by/handle/123456789/29040.

2 Прохвачева, О.Г. (2000) Лингвокультурный концепт "приватность": На материале американского варианта английского языка. Доступно через: http://www.dissercat.com/content/lingvokulturnyi-kontsept-privatnost-na-materiale-amerikanskogo-varianta-angliiskogo-yazyka#ixzz3AMsvTYM.

стве – наименованием *«свободных»* людей. В современных языках *«priyos»* отражено в понятиях *«приязнь»* и *«приятель»* в русском языке, freund и friend в немецком и английском языке, freedom и free в английском языке.

С другой стороны, латинские понятия proprius, privatus, suus связаны с индоевропейским *swe, греческмими ιδιωτης «частное лицо». Греческое Ιδιωτησ переводится на латинский язык как privatus, частное лицо, не выполняющее официальных обязанностей. Латинское «частная жизнь» *(vita privata)* аналогично греческому ιδιωτεία. Иными словами, *swe и его производные *(suus и др.)* говорят о выделении понятия *«себя»*, посредством которого человек пользуется, чтобы определить себя как индивида и «замкнуть происходящее на себя». Вместе с тем, *swe не ограничивается говорящим лицом, а предполагает в исходной точке узкую группу людей, *«своих»*, сомкнутую вокруг *«своего»*.

Латинское слово *«privatus»* – частный от *«privare»* – избавлять, лишать, отнимать и в этом смысле – освобождать, делать свободным. В современные беларусский, русский и украиснкий языки слово пришло из польского. В XVIII в. польское слово *«priwatny»* – *«приватный»* стало использоваться в значениях:

- *частный, необщественный;*
- *неофициальный, неслужебный;*
- *закрытый, недоступный для публичных оценок, конфиденциальный, секретный.*

В современном английском языке *«private»* трактуется как: 1) персональный, личный; секретный *(тайный)*; 2) предназначенный для отдельного человека или предпочитаемой, избранной группы, а не для каждого, не для общества, не для всех; 3) независимый; не связанный с правительством, государственной службой; 4) неофициальный; не связанный с другим делом или официальной позицией; с общественной жизнью; 5) *(место)*, где можно пребывать, находясь вне зоны видимости, слышимости и контроля со стороны других, внешнего мира; 6) *(о личности)* живущий частной жизнью.

В словарях русского и беларусского языков на первое место ставятся значения *«домашний»* и *«особенный»*. Значение, которое в словарях английского языка трактуется в общем виде как «не являющийся предназначенным и доступным для всех» обозначается как устаревшее. Между тем именно это значение указывает на ограничение доступа к чему-либо, а в словах типа *«домашний»* подразумевается *«неслужебная»* сторона жизни людей[1]. В связи с этим некоторые исследователи предлагают либо использовать слово *«прайвеси»*, которое используется в международных документах, как *«личное пространство»*. Наиболее *«экономным»* все же представляется актуализация устаревшего значения слова *«приватный»* (в значении *«частный, особенный, личный»*, противополагаемом значению *«общий, общественный, гласный»*: *«Дело приватных людей превратилось в дело государственное»*. Д. Фоннвизин, Торгующее дворянство, 1766 г.).

Термин *«прайвеси»* в Большом юридическом словаре (Большой юридический словарь. – М.: Инфра-М. А. Я. Сухарев, В. Е. Крутских, А.Я. Сухарева. 2003.) толкуется следующим образом: *«(англ. privacy – тайна, уединение, частная жизнь) – особая правовая категория в англо-американской правовой системе, означающая тайну и неприкосновенность частной жизни, интимную сферу человека. Термин «privacy» не имеет аналогов в русском языке. Он может означать в одних случаях частную жизнь, в других – право на частную жизнь, в-третьих – право на защиту неприкосновенности частной жизни и т.д.»*

1 Мельников, М. В. (2012) О семантике понятия "приватное" // XIII международная научная конференция преподавателей, аспирантов и студентов НСИ. С.181-189.

В данном курсе понятия «приватность» и «неприкосновенность частной жизни» рассматриваются как синонимичные. Термин «приватность» при этом представляется более предпочтительным, поскольку в меньшей мере акцентирует физические аспекты неприкосновенности личности.

ПРАВО НА ПРИВАТНОСТЬ (ПРАВО НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ)

Обеспечение права на неприкосновенность частной жизни (права на приватность) означает установление и соблюдение пределов допустимого вмешательства в частную жизнь.

Пределы допустимого вмешательства определяются:

физически – *границами между публичным и частным*, определяющими пространство, в которое организации, правительства или другие люди не могут вторгаться (здесь важно не забывать и о биометрических данных как «эквиваленте тела» индивида);

1. в сфере поведения – формами деятельности и образом действий, которые индивид имеет право защищать (скрывать) от внимания посторонних – *интимность*;
2. в сфере принятия индивидуальных решений – человек должен быть защищен от вторжения в эту сферу, то есть от давления на него при осуществлении индивидуального выбора – *свобода*;
3. возможностью человека *контролировать информацию о себе* - решать, когда, как и в каком объеме, информация о личности становится известной или сообщается другим[1].

Эти границы «частного» не абсолютны, а в значительной степени зависят от контекста, в рамках которого определяются нормы защиты частной жизни и требования того, что может и должно быть раскрыто для общества[2].

> *Проблема обеспечения права на приватность имеет, как минимум, три измерения: социально-этическое, политическое, инструментальное.*

Начиная рассуждать об уважении приватности и семейной жизни, необходимо принимать во внимание характер этого поколения прав человека, которые можно обозначить как определенные полномочия морального характера, как основные и универсальные этические принципы. Другими словами, речь идёт об определенном этическом идеале, на который должно опираться право.

Таким, образом, право на приватность, необходимо рассматривать в двух плоскостях.

- *право на приватность как ценность (философское содержание права, его обоснование и пределы);*
- *право на приватность как юридическая норма (причем эту норму нельзя рассматривать, не ссылаясь на философскую суть права на приватность).*

1 Westin, A. (1967) Privacy and Freedom. New York: Atheneum.
2 Schoeman, F. (1992) Privacy and Social Freedom. Cambridge, U.K.: Cambridge UniversityPress.

Право на приватность определяют границы автономии человека в современном обществе. При этом сфера частной жизни, прежде всего, должна быть свободна от вмешательства государственной власти (негативная обязанность государства). Вместе с тем государство должно эффективно защищать сферу автономии человека также от вмешательства со стороны других частных субъектов (позитивная обязанность государства)[1].

Проблема обеспечения права на приватность имеет, как минимум, три измерения: социально-этическое, политическое и инструментальное.

> *С социально-этической точки зрения* право на приватность предполагает защиту достоинства, индивидуальности, «личного пространства» человека[2]. Фундаментальная проблема здесь – недопущение потери индивидом достоинства, автономии, уважения вследствие утраты контроля над обстоятельствами, при которых возможно вторжение в реальное (физическое) и виртуальное (цифровое, телекоммуникационное) личное пространство, интимное поведение, принятие решений[3].
>
> *Политическое измерение* неприкосновенности частной жизни связано с тем, что автономия индивида – это одно из условий и существенных характеристик демократии, которое предполагает недопущение тотального полицейского надзора, свободу собраний, от контроля государства и пр.[4] П. Шварц охарактеризовал это измерение как «конститутивная неприкосновенность частной жизни» («constitutive privacy») в отношении защиты права индивидов на свободу слова и участия в общественной жизни онлайн[5].
>
> *Инструментальное измерение права* на приватность предполагает, что «правильные люди используют правильную информацию о личности в правильных целях», а индивид (субъект персональных данных) имеет возможность контролировать сбор, обработку, использование и раскрытие информации о себе[6].

ПРАВО НА ИНФОРМАЦИОННУЮ ПРИВАТНОСТЬ И ПРАВО НА ИНФОРМАЦИОННОЕ САМООПРЕДЕЛЕНИЕ

Право на информационную приватность – право индивида контролировать как саму информацию (объем и содержание), которая используется частными и государственными организациями, так и цели и способы ее обработки и распространения.

Право на информационную приватность – право индивида контролировать все информационные процессы, связанные со сбором и использованием персональных данных, независимо от того, какая персональная информация собиралась о нем

1 Килкелли, У. (2003) Право на уважение частной и семейной жизни. Гид по внедрению. Ст.8 европейской Конвенции по правам человека http://edu.helsinki.org.ua/library/privatlife/povaga-do-privatnogo-ta-s-meinogo-zhittya-na-zasadakh-st-8-vropeisko-konvents-pra.
2 Bennett, C. (2008) The Privacy Advocates: Resisting the Spread of Surveillance.. Massachusetts Institute of Technology. P.4.
3 Rule, J.et al. (1980) The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies. New York: Elsevier.
4 Westin, A. Op.cit.
5 Schwartz, P. (1999) 'Privacy and Democracy in Cyberspace. Vanderbilt Law Review 52, no. 6. PP 1610–1702.
6 Bennett, (2008, p.5.

частными и государственными организациями, так и способы ее обработки и распространения.

Понятие «информационная приватность» («informational privacy», «data privacy») вошло в словарь европейских экспертов в 1960 -1970-х гг. Расширение сферы компьютерной обработки данных, реализация проектов интеграции данных в национальных масштабах породили опасения относительно неограниченных возможностей для наблюдения, слежки и прослушивания. Стратегическая цель политики в этой сфере заключалась в том, чтобы предоставить индивиду возможности контролировать как саму информацию, которая собиралась о нем частными и государственными организациями, так и способы ее обработки и распространения.

Сформулированный в конце XIX в. подход к праву на приватность как к праву на контроль информации о себе был принят большинством политиков и правоведов, поскольку обеспечивал необходимую для правовой регламентации определённость, в отличие от трудностей интерпретации неприкосновенности частной жизни. Были высказаны предложения о конкретизации понятия посредством введения термина «неприкосновенность цифровой и телекоммуникационной сферы частной жизни»[1].

> *Право на приватность - это право индивида самостоятельно решать, когда, как и в каком объеме информация о нем может передаваться другим. (А. Уэстин)*

А. Уэстин определил право на приватность как право индивида самостоятельно решать, когда, как и в каком объеме информация о нем может передаваться другим[2].

Персональная информация рассматривается при этом как информация правдивая (в противном случае речь должна идти о диффамации или лжи) и конфиденциальная – то есть та информация, которую индивиды предпочитают не сообщать о себе (здоровье, зарплата, сексуальная ориентация и пр.).

В эпоху расширившихся возможностей обработки данных и объединения этих данных, конфиденциальность – достаточное, но не необходимое условие отнесения тех или иных сведений к персональной информации. Ведь сопоставление и установление связей даже между обезличенными данными позволяет идентифицировать индивида.

> *В августе 2006 г. компания «AOL» сделала общедоступными старые поисковые запросы, чтобы дать исследователям возможность анализировать их. Набор данных из 20 миллионов запросов от 650 00 пользователей за период с 1 марта до 31 мая 2006 г. был тщательно анонимизирован: личные данные (IP пользователя, имя и пр.) были удалены и замещены уникальным числовым идентификатором. Таким образом, исследователи могли связать между собой поисковые запросы одного и того же человека, но не имели информации о его личности. Тем не менее, в течение нескольких дней сотрудники издания «New York Times», связав поисковые запросы («одинокие мужчины за 60», «целебный чай» и «ландшафтный дизайнер в Лильбурне, Джорджия») установили, что пользователь № 4417749 – это Тельма Арнольд, 62-летняя вдова из Лильбурна, штат Джорджия[3].*

А. Уэстин выделяет 4 элемента права на информационную приватность:

- *право на одиночество;*
- *право на интимность;*

1 Вайхерт,Г. (2011) Защита персональных данных в рамках серии дискуссий «Настоящее будущего» Доступно через: https://www.datenschutzzentrum.de/vortraege/20110224-weichert-datenschutz-moskau-ru.pdf.

2 Westin, A. Op.cit.

3 Майер-Шенбергер, В. Кукьер, К.(2014) Большие данные. Революция, которая изменит то, как мы живем, работаем и мыслим. Москва: Манн, Иванов и Фербер. С. 161-162.

- *право на анонимность;*
- *право контролировать информации о себе.*

Границы информационной приватности подвижны и основаны на желании или нежелании индивида сообщать ту или иную информацию о себе[1].

> *В контексте права на информационную приватность анонимность определяется как функциональная неидентифицируемость персонального сообщения. Поэтому некоторые теоретики предлагают использовать термины «псевдонимность» или «неидентифицируемость». Однако эти предложения в целом не получили поддержки, и термин «анонимность» с соответствующими уточнениями остается наиболее употребительным. Как и другие составляющие права на приватность, анонимность не может быть абсолютной. В частности, пределы права на анонимность могут обуславливаться требованиями национальной безопасности или борьбы с правонарушениями.*
>
> *Право на информационную приватность – более широкое понятие, чем конфиденциальность, поскольку включает право на свободу от вторжений, право оставаться автономным и право управлять циркуляцией информации о себе. Право на конфиденциальность означает только защиту персональной информации, обычно в форме ограждения этой информации от несанкционированного раскрытия третьим лицам.*

Право на информационное самоопределение гарантирует возможность определять формат использования информации о себе

В 1980-х гг. было сформулировано понятие «информационного самоопределения» (Informationsselbstbestimmung), которое приобрело статус конституционного права в Германии[2]. В 1983 г. Федеральный конституционный суд ФРГ постановил, что все граждане имеют право на информационное самоопределение (возможность определять формат использования информации о себе):

> *«[…] в контексте современной обработки данных, защита индивидуума от неограниченного сбора, хранения, использования и раскрытие его/ее личных данных гарантируется общими правами личности, изложенными в Конституции. Это основное право гарантирует в данном отношении способность индивидуума определять в принципе раскрытие и использование его/ее личных данных. Ограничения этому информационному самоопределению допускаются только в случае серьезного затрагивания интересов общественности»»[3].*

Возможные ограничения этого права, подчеркнул суд, должны иметь законодательное закрепление и строгие административные процедуры санкционирования и осуществления.

Таким образом, право на информационное самоопределение включает:

- *право индивида самому решать, кто, что, когда и при каких обстоятельствах будет знать о нём/о ней;*
- *знание (прозрачность обработки данных);*
- *свободу выбора при обработке[4].*

1 Westin, A. Op.cit
2 Bennett, C. Op.cit.
3 Цит. по: Гачке, Л. (2009) Некоторые аспекты защиты прав потребителей при потребительском кредитовании. Доступно через: http://www.myshared.ru/slide/139127/.
4 Вайхерт,Г. (2011) Защита персональных данных в рамках серии дискуссий «Настоящее будущего». Доступно через: https://www.datenschutzzentrum.de/vortraege/20110224-weichert-datenschutz-moskau-ru.pdf.

ДАННЫЕ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ПОСЯГАТЕЛЬСТВО НА СФЕРУ ЧАСТНОЙ ЖИЗНИ

Термином «машинные данные» или просто «данные» обозначают информацию, полученную при цифровой обработке или подготовленную в специальной форме для такой обработки. Причины специального выделения категории «персональные данные» / «персонифицированные данные» из общего понятия «данные» связаны с тем, что такие данные являются потенциально уязвимыми атрибутами сферы частной жизни человека. В правовых документах ряда стран для обозначения таких данных используется термин «информация, на основании которой можно идентифицировать личность» (personally identifiable information)[1].

Раймонд Уэкс, профессор права Оксфордского университета, предлагает использовать термин «персональная информация»: «факты, сообщения или мнения, связанные с данным индивидом и относительно которых можно было бы ожидать, что он считает их интимными или конфиденциальными и, следовательно, желает прекратить или, по крайней мере, ограничить их распространение»[2].

В гражданском судопроизводстве стран общего права используется следующий принцип: публикация некоего факта частной жизни (персональных данных) признается посягательством на сферу частной жизни, если было доказано, что «публикация этого факта была крайне предосудительной с точки зрения любого благоразумного человека, наделенного обычной чувствительностью»[3]. Смысл этого судебного критерия в том, «что закон не предназначен для защиты сверхчувствительных людей, поскольку каждый человек должен до некого обоснованного предела открывать свою жизнь для пристального внимания общества»[4].

На основании этого информацию об индивидах подразделяют на две категории:

- *«нейтральные» персонифицированные данные, к раскрытию и распространению которых субъект данных относится индифферентно;*
- *данные, циркуляцию которых субъект данных стремится ограничить.*

Последняя категория получила название «персональные данные» и была квалифицирована как информация, несанкционированный доступ или ненадлежащее использование которой приводит к посягательствам на права субъекта данных[5].

В определениях понятия «персональные данные» используется, как правило, критерий идентифицируемости субъекта данных на основании этих данных

В определениях понятия «персональные данные» используется, как правило, критерий идентифицируемости субъекта данных на основании этих данных.

> Австрийский закон 1978 г. о защите данных: «Данные - информация, хранимая на носителе данных и имеющая отношение к некому идентифицированному

1 Gellman, R. (2014) Fair Information Practices: A Basic Histor». Доступно через: http://www.bobgellman.com/rg-docs/rg-FIPShistory.pdf.

2 Wakes, R. (1980) Protection of Privacy. London; Sweet & Maxwell. P. 31.

3 Судебное определение из дела “Диас против Окленд Трибюн, Инкорпорейтед” (139 Cal App3d 118, 1983). Цит. по: Warren Freedinan, Right of Privacy in Age of Computer. - L. - London, New York. 1986, p. 53.

4 Там же, p. 54.

5 Иванский, В. (1999) Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования. Доступно через: http://www.pravo.vuzlib.su/book_z137_page_1.html.

или могущему быть с высокой вероятностью идентифированным субъекту данных (персональные данные)»[1].

Датские законодательные акты 1979 г. о реестрах публичных органов власти и о частных реестрах определяют понятие «персональные данные» следующим образом: «Для целей настоящего законодательного акта термин «персональные данные» должен пониматься как обозначение данных, которые могут быть отнесены к идентифицируемым индивидуумам, даже если такое отнесение предполагает знание персонального регистрационного номера или любых подобных специальных средств идентификации такого индивидуума»[2].

Британский закон 1984 г. «О защите данных» вводит в определение дополнительные категории – «мнение» и «намерение»: Ст. 1(3). Термин «персональные данные» означает данные, состоящие из информации, связанной с неким живым индивидом, который может быть идентифицирован на основании этой информации (или с помощью этой и иной информации, находящейся в распоряжении пользователя данных), включая любое выражение мнения о данном лице, но без какого-либо указания о намерениях пользователя данных в отношении этого лица»[3].

Таким образом, любое выражение мнения об индивиде (субъекте данных) включается в состав персональных данных, тогда как любое указание на намерения пользователя данных в отношении субъекта данных однозначно исключается из категории «персональные данные» (необходимо подчеркнуть, что намерения третьей стороны, поскольку они в явной и недвусмысленной форме не исключены законом, включаются в состав персональных данных).

Другой важной особенностью британского определения является оговорка: «... или с помощью этой и иной информации, находящейся в распоряжении пользователя данных». Поскольку Великобритания разрабатывала свой закон о защите персональных данных почти на десятилетие позже других стран-участниц Конвенции 108 Совета Европы, то в законодательстве Великобритании была возможность учесть опыт применения аналогичных зарубежных законов. Приведенная выше оговорка призвана предупредить распространенную среди пользователей данных уловку: чтобы данные не подпадали под юрисдикцию законодательства о защите персональных данных, они хранят их в компьютере в псевдообезличенной форме - без упоминания идентифицирующих сведений о субъекте данных, но с привязкой к идентификационным кодам. Таблица же соответствия кодов и субъектов данных хранится (в ручной форме или на магнитных носителях) отдельно и при необходимости обеспечивает идентификацию субъектов данных этой якобы обезличенной компьютерной информации.

Исландский законодательный акт 1989 г. о регистрации и обращении с персональными данными распространяет понятие «персональные данные» и на сведения о юридических лицах (т.е. признает так называемое «корпоративное право на невмешательство в частную сферу»): «...к персональным данным относятся данные, связанные с частными, финансовыми или иными делами индивидов, институтов, компаний или иных юридических лиц, которые эти лица обоснованно должны держать в секрете»[4].

Определение из французского закона 1978 г. об обработке данных, файлах данных и индивидуальных свободах подчеркивает, что правовое регулирование обработки персональных данных распространяется как на публичный, так и на

1 Sec. 3(1) of Austrian Data Protection Act (1978).
2 Denmark Private Registers Act (1979) and Public Authorities Registers Act (1979).
3 Rec. 1(3) of UK Data Protection Act (1984).
4 Art. l of Act Concerning the Registration and Handling of Personal Data (1989, Iceland).

частный сектора. Ст. 4: «...персональные данные - это данные, которые позволяют в любой форме, прямо или косвенно, установить личность физического лица, в отношении которого эти данные собраны, независимо от того, физическими или юридическими лицами эти данные были обработаны»[1].

Особо следует отметить тщательную проработку определений персональных данных и смежных с ними понятий в финском законодательном акте 1988 г. о файлах персональных данных:

«1. Термин «персональные данные» означает любое описание любого физического лица или характеристик физического лица, или жизненных обстоятельств, которое может быть признано описывающим определенное частное физическое лицо или его семью или тех, кто живет с ним в одном и том же жилище.

2. Термин «файл персональных данных» означает любой набор данных, содержащий персональные данные, обработанные при помощи компьютера, а также любой перечень, картотеку или иной набор данных, содержащий персональные данные и организованный соответствующим образом, благодаря которому данные о любом конкретном физическом лице могут быть найдены легко и без чрезмерных затрат.

2а. Термин «файл редакционных данных» означает любой файл персональных данных, предназначенный только для редакторских операций любого члена редакции средств массовой информации и недоступный для посторонних.

6. Термин «персональные кредитные данные» означает персональные данные, предназначенные для использования при оценке финансового состояния физического лица, его способности соответствовать своим обязательствам или степени оказываемого ему кредитного доверия.

7а. Термин «матрикула» означает любой файл персональных данных, предназначенный для публикации, в который физические лица входят вместе со сведениями о конкретной профессии или образовании, членстве в некой профессиональной организации или ином обществе, со своим статусом или достижениями в области культуры, спорта, экономической жизни или иной гражданской деятельности или в соединении с другими сопоставимыми факторами»[2].

Этот законодательный акт, относящийся к так называемым «законам второго поколения», учитывает опыт применения предыдущих отечественных и зарубежных законов и содержит ряд принципиально новых моментов. Пункт 1 распространяет понятие «персональные данные» на сведения о семье субъекта данных и о тех, «кто живет с ним в одном и том же жилище». Пункт 2 выводит понятие «персональные данные» за пределы чисто компьютерной информации, распространяя его на данные в информационных системах иных технологий (ручных, механических и т.д.). Принципиальной новинкой является определение «отраслевых» персональных данных в пунктах 2а, 6 и 7а (для кредитной отрасли и для средств массовой информации). Особенно важным представляется появление в законе определений терминов «файл редакционных данных» и «матрикула», поскольку после внедрения компьютерных технологий в повседневную работу печатной и электронной прессы обработка персональных данных в средствах массовой информации стала объектом правового регулирования одновременно со стороны деликтных средств правовой защиты сферы частной жизни от посягательств в форме несанкционированных публикаций или публичной огласки, сформировавшихся в «докомпьютерную эпоху», и со стороны правовых институтов, регулирующих отношения в информационной сфере. Проработка в законе

1 Sec.4 of Act on Data Processing, Data Files and Individual Liberties (1978, France).
2 Sec.2 of Personal Data File Act (1988, Finland).

таких определений способствует тому, чтобы взаимоотношения деликтного и информационного права в этой точке соприкосновения сфер их правового регулирования были не конкурентными, а взаимно дополняющими.

ЧУВСТВИТЕЛЬНЫЕ / УЯЗВИМЫЕ ДАННЫЕ

В национальных законах о защите данных в определении «персональные данные», в свою очередь подразделяются по критерию «чувствительности»/ «уязвимости»). При этом национальный закон о защите персональных данных либо содержит прямое указание на отнесение данных к определенной категории, либо наделяет представителей государственной власти (как правило, министра, курирующего национальный орган по защите данных, иногда премьер-министра) полномочиями принятия оперативных решений по данному вопросу[1].

По критерию чувствительности/уязвимости персональные данные подразделяются на три категории

- *«обычные» персональные данные - их сбор, обработка, использование и передача возможны без специального разрешения в режиме, предписанном национальными законами;*
- *«чувствительные» персональные данные - их сбор, обработка, использование и передача требуют особых мер защиты и безопасности, специально установленных законом;*
- *«особо чувствительные» персональные данные - их сбор, обработка, использование и передача либо вообще запрещены законом, либо разрешены только в исключительных случаях с использованием специальных мер защиты и безопасности.*

К категории чувствительных / уязвимых персональных данных относятся сведения об арестах, банковские данные, данные кредитных отчетов и кредитной истории, данные об образовании и трудовой деятельности (как правило, только данные, содержащие оценку способностей и трудовых качеств индивида), медицинские данные, налоговые данные и т.п.

В соответствии с бельгийским законодательством, медицинские данные (чувствительные данные) контролер файлов может обрабатывать только после заблаговременного получения письменного разрешения субъекта данных или, в качестве альтернативы, под строгим надзором и при ответственности лечащего врача. В категорию медицинских включаются все данные, раскрывающие информацию, связанную с предыдущим, текущим или будущим состоянием физического или умственного здоровья субъекта данных, за исключением данных явно административного или оценочного характера, относящихся к способу лечения и медобслуживания. Медицинские данные не могут передаваться третьим сторонам, за исключением тех случаев, когда это делается во исполнение закона, или когда закон содержит явно выраженное и недвусмысленное разрешение на такую передачу. Медицинские данные также могут передаваться другим лечащим медработникам после получения заранее специального письменного разрешения от заинтересованного лица (субъекта данных) или для целей

1 Иванский, В.Op.cit.

медицинской обработки в чрезвычайных ситуациях и в случаях опасности (ст. 7 закона Бельгии «О защите данных»).

К чувствительным относятся уголовные и судебные персональные данные, которые могут обрабатываться только во исполнение закона или для целей, определенных законом. Причем в эту категорию включается обработка данных об уголовных обвинительных приговорах и наказаниях из документов, хранимых в национальных архивах уголовных дел, а также обработка данных из уголовных документальных записей, хранимых муниципалитетами (ст. 8, § 4). Обработка таких данных адвокатами (ст. 8, § 6) и юридическими лицами, уполномоченными на то королевским указом, - во всех этих случаях обработчик данных обязан заранее посылать субъекту данных уведомление о предстоящей обработке относящихся к нему уголовных данных[1].

Набор «особо чувствительных» персональных данных, подлежащих тщательной защите, может варьироваться в различных странах, но, как правило, к этой категории относятся данные о расовом и этническом происхождении, религиозных верованиях, политических убеждениях, членстве в профессиональных ассоциациях, политических и общественных организациях, состоянии здоровья, особенностях сексуального поведения, криминальном прошлом (данные о вынесенных и исполненных обвинительных судебных приговорах по уголовным делам).

В соответствии с бельгийским законодательством должны соблюдаться особо строгие правила обработки и использования в отношении следующих данных, считающихся особо чувствительными (бельгийский законодательный акт 1992 г. о защите данных (BDPA)): данные , связанные с расой, этническим происхождением, сексуальным поведением, политическими взглядами или действиями, религиозными или философскими убеждениями, членством в любом профессиональном или трудовом союзе или принадлежностью к государственной службе здравоохранения. Любой контролер файлов может обрабатывать эту категорию чувствительных данных только для целей, разрешенных BDPA, или во исполнение этого законодательного акта. Поскольку сам BDPA не предусматривает никаких разрешенных целей для обработки чувствительных данных, то эти цели в деталях устанавливаются королевскими указами № 6 и 7, конкретизирующими и регламентирующими исполнение вышеуказанного законодательного акта. BDPA допускает исключения для юридических лиц и организаций де-факто (таких, как профсоюзы, службы здоровья, политические партии), но только в отношении данных, связанных с их собственными членами[2].

ОСОБО ОПАСНЫЕ ИНФОРМАЦИОННЫЕ ОБЪЕКТЫ

К особо опасным информационным объектам относятся базы и банки данных, пространственно-распределенные информационные системы со сверхвысокой концентрацией персонифицированной информации, программные процедуры типа «data matching» (процедуры сопоставления/состыковки файлов персональных данных) и т.п.

В ряде стран существуют строгие ограничения, не допускающие применения процедур типа «data matching» даже в рамках одной и той же базы данных, за исключением случаев, прямо предусмотренных законом.

1 Подробно об этом см. Иванский, В. Op.cit.
2 Там же

Бельгийский закон 1992 г. о защите данных не содержит запрета, ограничения или иной регламентации совмещения (объединения) персональных данных из разных файлов (что принято называть автоматическим «согласованием» персональных данных и банков данных). Он оставляет детальную регламентацию на долю специальных королевских указов, предусматривая в ст. 21 возможность наложения запретов или ограничений (например, таких, как предварительное санкционирование каждого случая «согласования данных») на определенные категории процедур типа «data matching» или установление иных взаимосвязей между персональными данными1.

Канада. Личный номер социального страхования (ЛНСС) был впервые введен в Канаде в 1936 г, для использования при сборе налогов, выплате пенсий и социальных пособий. Однако многие федеральные нормативные правовые акты санкционируют использование ЛНСС в качестве единого персонального универсального идентификатора личности. Например:

- *законодательный акт «О сборе подоходных налогов»;*
- *законодательный акт «О проведении всеобщих выборов в Канаде»;*
- *законодательный акт «О социальном страховании по безработице»;*
- *Инструкции Канадского пенсионного фонда;*
- *Инструкции о социальном страховании по старости;*
- *Инструкции о социальном страховании по безработице;*
- *Инструкции о выплате пособий ветеранам и т. д.*

Для предотвращения посягательств на сферу частной жизни Канадское федеральное правительство разработало план работы по контролю за «согласованием данных» и ограничению использования личного номера социального страхования в качестве персонального идентификатора. Этот план требует, чтобы правительство информировало Федерального специального уполномоченного по защите прав граждан на неприкосновенность частной жизни о всех реализуемых программах по «согласованию данных» и публиковало отчеты о них для обеспечения контроля со стороны общества. Все собранные в рамках таких программ данные должны подвергаться перепроверке с привлечением субъектов данных. Граждане должны быть осведомлены о цели запроса их ЛНСС во время любой процедуры сбора информации и, если это особо не оговорено законом, правительственные учреждения не вправе отказывать в услугах из-за нежелания граждан предоставлять информацию о своих персональных идентификационных номерах. Законоположения, регламентирующие использование процедуры «согласования данных» и персонального идентификатора, имеются в законодательных актах о защите прав граждан на неприкосновенность частной жизни ряда провинций Канады, а контроль за их исполнением возлагается на Уполномоченных провинций по защите прав граждан на неприкосновенность частной жизни.

Дания. Датские органы законодательной власти, ввиду увеличения использования персональных идентификационных номеров, в 1987 г. внесли специальные поправки в закон 1979 г. «О частных реестрах», более детально регламентирующие «регистрацию» (этим термином вышеупомянутый закон определяет занесение данных в компьютерные файлы) той информации, которая включает в себя персональные номера. В частности, «регистрация» персональных номеров не может теперь осуществляться частными предприятиями.

США. В США Национальные идентификационные номера социального обеспечения (CCIN), присваиваемые почти каждому индивиду, давно уже обрели характер универсального идентификатора, и в публичной сфере почти не осталось уже ведомств и учреждений, которые не пользовались бы этим удобным

(но, по вышеизложенным причинам, опасным) инструментом для идентификации граждан. Федеральное правительство пыталось ограничить чрезмерное использование номеров CCIN, требуя, чтобы федеральные, местные учреждения и учреждения штатов извещали каждого индивида о правовом основании, которое позволяет им при выполнении их функций, в числе прочей информации, требовать от индивида указания его номера CCIN, а также устанавливает, какое использование может быть придано этим номерам (ст. 552a (7) Свода законов о гражданских правонарушениях). Однако законодательный акт 1976 г. «О налоговой реформе» снял это ограничение с ведомств штатов, которые занимаются социальным обеспечением, налогами и автомобильным транспортом. Тем не менее, согласно ст. 26 USC 408, существуют уголовные наказания за раскрытие или использование номера CCIN любого человека вопреки федеральному закону. В соответствии с законодательством штата Вирджиния незаконно: (1) требовать от человека сообщения его номера CCIN для совершения любого юридического акта или сделки; (2) отказывать в услуге или обслуживании, если номер CCIN не был сообщен, если только раскрытие идентификационного номера не требуется федеральным законом или законом штата (Кодекс штата Вирджиния, ст. 2. 1-385). Однако та же самая Вирджиния требует указания номера CCIN на водительских лицензиях резидентов штата Вирджиния (ст. 46.1-375); кроме того, избиратели в штате Вирджиния, чтобы проголосовать, должны раскрывать свои номера CCIN (ст. 24. 1-72. 2)[1].

БОЛЬШИЕ ДАННЫЕ И МЕТАДАННЫЕ

Сегодня в мире накоплено столько информации, что на каждого живущего приходится в 320 раз больше того набора данных, который, как считают историки, хранился в александрийских фолиантах – ее объем оценивается в 1200 эксабайтов (квадриллионов килобайтов). Если все это поместить на CD-диски, которые затем разложить в пять стопок, то каждая из них будет высотой до Луны. Еще в 2000 г. лишь четверть всех накопленных в мире сведений была оцифрована. Остальное хранилось на бумаге, пленках и других аналоговых носителях. Но поскольку объем цифровых данных быстро увеличивается, удваиваясь каждые три года, положение дел быстро меняется, и сегодня неоцифрованной остается менее 2% всей хранящейся информации.

С учетом этого гигантского масштаба возникает искушение рассматривать большие данные исключительно с точки зрения их размера. Но это может сбить с толку. Большие данные способны обращать в «цифру» то, что никогда раньше не оценивалось количественно: назовем это датификацией (datafication). Например, местоположение объекта на поверхности Земли стало возможным датифицировать сначала с открытием долготы и широты, а сравнительно недавно – с изобретением спутниковых систем GPS. Слова превращаются в цифры, когда компьютеры раскапывают в старинных книгах наслоения эпох. Даже дружеские отношения и симпатии датифицируются через Facebook («лайки»).

Для этого вида данных возможны новые способы применения с помощью мощных процессоров, умных алгоритмов, программного обеспечения и математики, которая заимствует цифры из фундаментальной статистики. Вместо того чтобы пытаться обучить компьютер вождению автомобиля или переводу с одного языка на другой, над чем специалисты по искусственному интеллекту безуспеш-

1 Там же

но бились десятилетиями, новый подход заключается в закачивании достаточно большого объема данных в компьютер. В результате выводится вероятность того, что светофор даст зеленый, а не красный свет, или что в определенном контексте «lumiere» – ближе по значению к понятию «свет», чем «leger».

Подобное использование информационного массива требует трех глубоких изменений в наших подходах. Первое заключается в подборке из множества данных, когда люди уже не довольствуются небольшими объемами или выборками, как более 100 лет назад начали делать специалисты по статистике. Второе – отказ от предпочтительного использования кристально чистых и проверенных данных в пользу естественного беспорядка: все большее число сценариев и ситуаций допускает некоторую неточность, поскольку большой поток разного качества эффективнее и менее затратен, чем ограниченная выжимка очень точных сведений. В-третьих, во многих случаях нам придется отказаться от поиска причин и принять на вооружение непричинные виды детерминации. Вместо того чтобы пытаться точно понять, почему ломается двигатель или исчезает побочный эффект какого-то лекарства, исследователи могут собирать и анализировать большие массивы информации об этих вещах и явлениях и обо всем, что с ними связано, в поиске стереотипов и шаблонов, которые помогут предсказывать их появление сегодня или в будущем. То есть отвечать на вопрос «что?», а не «почему?», но часто этого достаточно[1].

Термином «большие данные» определяется не столько объем данных, а характеристики наборов данных. Эти характеристики часто обозначают аббревиатурой 3 V (Volume, Velocity, Variety):

- *объем (Volume) то, что нецелесообразно или неудобно обрабатывать на одной машине и нужно «распараллеливать» для обработки;*
- *скорость поступления (Velocity), которая также диктует «параллельную» обработку;*
- *неструктурированность, разнообразие форматов (Variety) – такие данные, которые не могут храниться в классических базах данных[2].*

Как известно, возможность искажения данных растёт вместе с их объемом, и в случае «больших данных» искажения могут стать критическими. Поэтому «большие данные» следует рассматривать как ресурс и инструмент, призванный скорее информировать, чем объяснять. Они ведут к пониманию разных явлений, но иногда провоцируют ошибочные выводы – все зависит от того, как их использовать. Но какой бы яркой и ослепительной ни казалась власть «больших данных», их обманчивая мишура и привлекательность не должны затмить присущие им несовершенства. Принимая и используя технологию, нельзя забывать о ее ограничениях[3].

В эпоху «больших данных» ценность персональной информации не очевидна во время её сбора, когда даётся уведомление и согласие.

В эпоху «больших данных» ценность персональной информации не очевидна во время её сбора, когда даётся уведомление и согласие.

Если бы использование информации требовало повторного согласия, это было бы очень затратно. Более того, некогда сравнительно простые отношениями между

1 Майер-Шёнбергер, В., Кейт, Ф. (2013) Уведомление и согласие в мире больших данных. Доступно через: http://webscience.ru/details/uvedomlenie-i-soglasie-v-mire-bolshih-dannyh.

2 Клозариди, П. (2013) Большие данные, кому они могут пригодиться. Доступно через: http://webscience.ru/details/bolshie-dannye-kak-oni-menyayut-nashi-predstavleniya-o-mirehttp://webscience.ru/details/bolshie-dannye-komu-oni-mogut-prigoditsya.

3 Майер-Шёнберге, В, Кукир, К. Большие данные. Как они меняют наши представления о мире. Доступно через: http://webscience.ru/details/uvedomlenie-i-soglasie-v-mire-bolshih-dannyh.

теми, кто предоставляет информацию и теми, кто использует или обрабатывает её, затрудняется по мере объединения массивов данных и изменения компаний, имеющих к ним доступ. Ведь «большие данные» собираются и обрабатываются так часто, что для большинства людей крайне неудобно каждый раз заново давать свое согласие. В качестве иллюстрации можно привести всего один пример:

> *Газета «Нью-Йорк Таймс» сообщила в 2012 году, что одна американская компания, о которой мало кто слышал, в одном только 2012 году совершила более 50 триллионов операций с использованием зарегистрированных персональных данных*[1].

Метаданные - это данные о данных, информация об информации, описание контента.

Хранение и доставка информации в электронном виде порождает много проблем. Пользователи должны иметь возможность найти нужную информацию, получить доступ к ней в приемлемой для них форме. Создатели информации должны быть уверены, что их права на интеллектуальную собственность будут защищены, а администраторы и иные специалисты должны иметь возможности по сопровождению электронной информации, например, обеспечение ее сохранности в течение длительного времени. Метаданные являются ключевым компонентом для решения этих проблем. Учитывая, что значительная часть служебных задач может решаться и реально решается без участия человека, метаданных подразделяют на предназначенные для использования приложениями и для использования человеком (machine-readable и human-readable).

Существуют различные классификации метаданных, отличающиеся между собой, главным образом, степенью детализации. Чаще их подразделяют на две большие группы:

- *метаданные описания контента;*
- *административные метаданные.*

Контентные метаданные охватывают описание всех аспектов данного информационного объекта как отдельной сущности. Иногда их дополнительно подразделяют на структурные и описательные.

Административные метаданные объединяют различные группы и отличаются большим разнообразием:

- *позволяют владельцу ресурса проводить четкую и гибкую политику в отношении информационного объекта, включая авторизацию, аутентификацию, управление авторскими правами, доступом, а также служат для идентификации и категоризации объектов в рамках специальной коллекции или организации;*
- *могут включать в себя не только метаданные, необходимые для нахождения ресурсов, возможные правила и условия доступа и т.д., но и периоды времени для классифицированной информации, информацию об открытом или закрытом хранении, данные об использовании, историю миграции с одной программно-аппаратной платформы на другую и т.д.;*
- *используются для позиционирования данного информационного ресурса в контексте группы подобных документов, информационно-поисковой системы, предметной области и т.д.;*
- *метаданные можно использовать для кодирования содержательной информации о том, для каких групп пользователей предназначен ресурс, для ориенти-*

1 Там же.

рования пользователей относительно его философского, мировоззренческого смысла;

- *поскольку могут существовать и реально существуют различные наборы метаданных, возникает потребность в специальных форматах обмена метаданными между различными информационными системами.*

Правительство является одним их самых больших владельцев информационных ресурсов. Поэтому он несет ответственность за обеспечение увеличения ценности этих ресурсов для граждан, предприятий, правительственных должностных лиц и пользователей по всему миру.

Оно также отвечает за обеспечение возможности поиска, доступа и передачи информации между общественным и частным секторами, сохраняя требования частного использования и конфиденциальности информации. Таким образом, наличие хорошо структурированного и постоянно применяемого стандарта метаданных становится все более и более важным для правительства; такой стандарт может помочь людям совершать поиск в большом количестве веб-страниц с информацией и уверенно определять местонахождение искомого ими.

В процессе коммуникации можно получить следующие данные о данных:

- *информацию о клиенте;*
- *информацию об устройстве;*
- *происхождение и направление коммуникаций (посещаемые вебсайты, скачанные и просмотренные материалы);*
- *контакты;*
- *поиск;*
- *использованные ресурсы;*
- *местонахождение.*

Объем данных о данных позволяет не только идентифицировать индивида, но и узнать о нем практически все.

ЗАЩИТА ЦИФРОВОЙ СФЕРЫ ЧАСТНОЙ ЖИЗНИ

Защита персональных данных как цифровой сферы частной жизни - основная потребность человека в современном информационном обществе [1]

Понятие «защита персональных данных» не сводится к требованиям обеспечения качества и безопасности обработки данных, поскольку включает и защиту права субъекта персональных данных контролировать эти данные. Такая узкотехническая трактовка термина «защита персональных данных в политическом и юридическом дискурсах не может считаться корректной.

Защита прав субъектов персональных данных обеспечивает право на информационную приватность, поскольку защищает любые данные или объединение данных, на основании которых может быть идентифицирована личность (персона), то есть «информационную составляющую частной жизни человека»

1 Вайхерт, Г. (2011) Защита персональных данных в рамках серии дискуссий «Настоящее будущего». Доступно через: https://www.datenschutzzentrum.de/vortraege/20110224-weichert-datenschutz-moskau-ru.pdf.

Понятие «персональные данные» в широком смысле включает факты, сообщения или мнения, связанные с определенным индивидом и относительно которых разумно было бы ожидать, что он считает их интимными или конфиденциальными, и, следовательно, не желает предавать их огласке или, по крайней мере, желает ограничить их обращение. С этой точки зрения «защита персональных данных» может считаться своего рода аналогом термина «информационная приватность» и в этом смысле предполагает право индивидов решать, когда, какая и в каком объеме информация о них может сообщаться другим.

Понятия «сведения, составляющие тайну индивида» и «персональные данные» не являются идентичными. Персональные данные (такие как, к примеру, фамилия, имя, отчество, образование, профессия) личной тайны не содержат, но позволяют идентифицировать того или иного человека. Отсюда определение персональных данных в узком смысле – любые данные или совокупность данных, которые позволяют идентифицировать индивида.

Обеспечение защиты прав субъектов персональных данных подразумевает не только предотвращение злоупотреблений при обработке информации, но и защиту права на информационное самоопределение.

ЗАЧЕМ ЗАЩИЩАТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ?

В будущем, к которому мы движемся, опасность будет исходить не от всезнающего «Большого брата», отслеживающего и записывающего каждый наш шаг, а от сотен «маленьких братьев», постоянно подглядывающих и вмешивающихся в нашу жизнь. Джордж Оруэлл считал, что главная угроза свободе индивидуальности исходит со стороны коммунистической системы. Но за последние 50 лет мы увидели новые виды угроз приватности, корни которых уходят совсем не в тоталитаризм, эти угрозы выросли на почве свободного капиталистического рынка, современных технологий и неконтролируемого обмена электронной информацией[1].

Саймон Гарфинкель, автор книги «Все под контролем: Кто и как следит за тобой», писал: «В будущем, к которому мы движемся, опасность будет исходить не от всезнающего «Большого брата», отслеживающего и записывающего каждый наш шаг, а от сотен «маленьких братьев», постоянно подглядывающих и вмешивающихся в нашу жизнь. Джордж Оруэлл считал, что главная угроза свободе индивидуальности исходит со стороны коммунистической системы. Но за последние 50 лет мы увидели новые виды угроз приватности, корни которых уходят совсем не в тоталитаризм, эти угрозы выросли на почве свободного капиталистического рынка, современных технологий и неконтролируемого обмена электронной информацией[2].

И действительно, угрозы информационной приватности разнообразны. Они порождаются применением новых цифровых и телекоммуникационных технологий и связаны со сбором, хранением, и обработкой информации частными и государственными структурами, киберпреступностью, некорректным поведением пользователей интернета, а также мерами, предпринимаемыми правительствами в целях обеспечения национальной безопасности, и т.п.

Эти угрозы реализуются в:

- *ненадлежащих способах сбора информации (массовое систематическое слежение, перехват сообщений, опросы, анкеты и пр.);*
- *несоблюдении необходимых мер защиты при обработке информации;*
- *ненадлежащих способах распространения информации (нарушение конфиденциальности, разглашение, предоставление доступа, присвоение, искажение информации и др.);*
- *вмешательстве – непосредственном влиянии на личность, на поведение субъекта данных*[3].

Однако основная проблема заключается в том, что новые технологии создают беспрецедентные возможности для сознательного или неосознанного нарушения информационной приватности.

1 Гарфинкель, С. (2003) Все под контролем: Кто и как следит за тобой. Доступно через: http://www.uhlib.ru/kompyutery_i_internet/vse_pod_kontrolem_kto_i_kak_sledit_za_toboi/index.php.
2 Там же.
3 Солоув, Д. «Мне нечего скрывать» и другие ошибочные толкования приватности. Доступно через: https://www.pgpru.com/biblioteka/statji/nothingtohide.

Однако основная проблема заключается в том, что новые технологии создают беспрецедентные возможности для сознательного или неосознанного нарушения информационной приватности.

Угрозы приватности – проблема любых баз персональных данных, которая проистекает из различия между физической и электронной формой представления. Физической формой являются записи на бумажном носителе. Они могут существовать в данный момент времени лишь в одном месте. Чтобы отправить копию этих записей по факсу, человек должен иметь к ним физический доступ. Основное преимущество электронных записей заключается в том, что ими легко манипулировать, но эта легкость опасна: *поскольку к компьютерному файлу можно получить доступ одновременно с сотен терминалов, задача контроля становится чрезвычайно сложной.*

В отчете, опубликованном в 1997 г. Национальным советом по исследованиям США, выделено пять «уровней угроз» информации, хранимой в медицинских компьютерах:

- *инсайдеры (законные пользователи системы), которые совершают «невинные» ошибки, приводящие к случайному разглашению конфиденциальной информации. Это могут быть такие простые ситуации, как посылка результатов лабораторного исследования по факсу на ошибочный номер или передача медсестрой записей одного пациента вместо другого;*
- *инсайдеры, превышающие свои полномочия по доступу к информации. Просмотр является распространенной проблемой во многих электронных системах хранения информации. В Налоговом управлении всегда существовала проблема любопытных служащих, просматривающих налоговую документацию, к которой они имели доступ. Было бы наивным полагать, что госпитали могут так или иначе избежать этой беды;*
- *инсайдеры, которые осуществляют доступ к информации со злым умыслом или с целью наживы. С. Гарфункель приводит такой пример: «Во время предвыборной кампании Демократической партии в 1992 году к одному моему знакомому патологоанатому из госпиталя Берта Израэля в Бостоне обратился представитель прессы, желавший получить доступ к медицинским данным кандидата Пола Цонгаса. Репортер предложил неплохие деньги, и менее этичный врач мог бы легко достать нужный файл, не оставив при этом следов»;*
- *физический нарушитель, получивший доступ к информации, не имея на это права. Многие госпитали полагаются на физические меры обеспечения безопасности хранимой в компьютерах информации: терминалы размещаются в специальных помещениях или за стойками, куда должен иметь доступ только допущенный персонал. Но журналист мог просто надеть белый халат, фальшивую табличку с именем и получить доступ к данным Цонгаса без посторонней помощи;*
- *обиженные служащие и внешние нарушители, такие как желающие отомстить пациенты или нарушители, планирующие несанкционированный доступ к информации, повреждение систем или прерывание операций. Вот еще один пример С. Гарфункеля. Один из служащих проникал в компьютер, на котором хранилось расписание работы врачей, и удалял записи о назначенных визитах пациентов. В регистратуре думали, что данное время свободно и назначали его для других; в результате на прием одновременно являлось два или три пациента.*

Ошибки, возникающие в результате объединения данных различных государственных структур – источник серьезных угроз информационной сфере частной жизни. Существует мнение, что более половины наборов сведений о гражданах, которые

собирают правительства, содержат ошибки. Некоторые из этих ошибок, такие как неправильный адрес, несущественны, их легко заметить и исправить. В других случаях может совместиться кредитная информация о двух совершенно разных людях с похожими именами и т.п. Тогда довольно сложно бывает понять основания тех или иных решений, принимаемых соответствующими учреждениями.

Массовая систематическая слежка за гражданами – одна из серьезнейших угроз неприкосновенности частной жизни онлайн.

Необходимые технологические предпосылки для создания всеобъемлющей компьютерной системы слежения за частной жизнью каждого индивида были созданы еще в 1970-х гг.

> Первая интернет-видеокамера была установлена в 1991 году в компьютерной лаборатории Кембриджского университета и показывала кофейник в «Троянской комнате». Пятнадцать аспирантов пользовались одним кофейником, расположенным на втором этаже лаборатории, называемой «Троянская комната». Кофейник был удобен для аспирантов, работающих на втором этаже. Проблема заключалась в том, что аспиранты на других этажах не знали, когда будет готов кофе. Конечно, они были слишком заняты (и немного ленивы), чтобы пойти на второй этаж, включить кофейник и подождать, пока кофе приготовится. Они хотели знать, когда кто-нибудь другой в здании возьмет на себя тяжкий труд включить кофейник, чтобы после быстренько налететь и насладиться кофе.
>
> Аспиранты нашли старую видеокамеру и вспомогательный компьютер с устройством ввода видеосигнала. Пол Джардецки написал программу, которая получала изображение с устройства ввода видеосигнала каждые несколько секунд. Квентин Стаффорд-Фрейзер написал другую программу под названием «XCoffee», которая связывалась с программой Джардецки по сети и выводила изображение кофейника на экран компьютера. «Картинка обновлялась всего лишь три раза в минуту, но это было неплохо, так как кофейник наполнялся довольно медленно; она была также черно-белой, что тоже было достаточно», – писал Стаффорд-Фрейзер на веб-странице, посвященной проекту.
>
> Кофейник стал приобретать некоторое количество поклонников по всему миру. Боб Меткальф написал о нем в выпуске «Comm Week» от 27 января 1992 года. Как он сообщал, копию «XCoffee» загрузили 600 человек, которые теперь тоже могли наблюдать кофейник. Но программа работала только на рабочих станциях под управлением системы «UNIX», что несколько ограничило ее распространение. Когда вспомогательный компьютер внезапно вышел из строя, аспиранты Дэниэль Гордон и Мартин Джонсон возродили систему на новом оборудовании и поместили изображение кофейника непосредственно на свою веб-страницу.
>
> Это привело к существенным изменениям. До расцвета Всемирной паутины, единственным способом увидеть кофейник в «Троянской комнате» было загрузить программу «XCoffee» и запустить ее. Поскольку программа имела только одну функцию, то сомнительно, что результат оправдывал затраченные усилия. Другая проблема была в том, что «XCoffee» могла работать только на некоторых типах рабочих станций «UNIX». Но помещение изображения на веб-страницу привело к тому, что любой обладатель браузера мог просмотреть его путем простого щелчка мышью на ссылке. Браузер не нуждался в специальной модификации для показа изображения: с точки зрения браузера, нет никакой разницы между изображением кофейника и фотографией президента США на веб-странице Белого дома.
>
> Работа Гордона принесла результат: согласно сообщению BBC, 11 ноября 1994 года более 150 тысяч человек активировали ссылку на кофейник в «Троянской

> комнате» с момента первого появления изображения во Всемирной паутине. Это было рождением веб-камер[1].

Сегодня видеокамеры постоянно присутствуют в окружающем нас мире. Они установлены в магазинах, в учреждениях, на улицах и в квартирах. Возможность массивного всеохватывающего контроля государства за частной жизнью индивидов получила неофициальное, но практически повсеместно распространенное название «проблемы Большого брата».

Суть функционирования системы массового систематического слежения сводится к процедуре поиска и выборки персональных данных конкретного субъекта из различных файлов (которые могут храниться в компьютерных банках данных, дислоцированных в разных концах страны) и слияния этих персональных данных в единый файл, содержащий исчерпывающие сведения о данном субъекте данных (data matching – совмещение, стыковка, согласование данных). Создание системы «Большого брата» на базе применения процедур типа «data matching» предполагает наличие единого поискового признака – универсального идентификационного кода.

С. Гарфункель так охарактеризовал изменения, связанные с распространением систем скрытого видеонаблюдения (CCTV): «В прошлом прогуливаясь в одиночестве по городским улицам или беседуя с другом в парке, люди ощущали себя защищенными от пристального внимания «чужих глаз». Но постоянный мониторинг изменил эти представления на прямо противоположные. Мы справедливо полагаем, что приватность гарантируется нам дома, но мы не строим таких же предположений относительно общественных мест. И чем больше все происходящее фиксируется, записывается, индексируется и легко извлекается на свет при необходимости, тем меньше приходится рассчитывать на анонимность в общественных местах» [2].

> *В прошлом прогуливаясь в одиночестве по городским улицам или беседуя с другом в парке, люди ощущали себя защищенными от пристального внимания «чужих глаз». Но постоянный мониторинг изменил эти представления на прямо противоположные. Мы справедливо полагаем, что приватность гарантируется нам дома, но мы не строим таких же предположений относительно общественных мест. И чем больше все происходящее фиксируется, записывается, индексируется и легко извлекается на свет при необходимости, тем меньше приходится рассчитывать на анонимность в общественных местах. (С. Гарфункель)*

«Объективность» того, что фиксируют видеокамеры CCTV подвергается обоснованным сомнениям.

Основатель международной неправительственной организации «Privacy International» Саймон Дэвис на слушаниях в Палате лордов в 1997 г. по вопросу воздействия постоянного видеонаблюдения заявил:

- *«Непредвзятость этой технологии показная, непроверенная и основывается в значительной степени на эмоциональных соображениях. Заявления о влиянии систем CCTV на уровень и состав преступлений часто преувеличены и упрощены. Например, преступления на почве ревности, преступления, связанные с наркотиками и алкоголем, и действия профессиональных преступников редко*

1 Гарфинкель, С. (2003) Все под контролем: Кто и как следит за тобой. Доступно через: http://www.uhlib.ru/kompyutery_i_internet/vse_pod_kontrolem_kto_i_kak_sledit_za_toboi/index.php.

2 CCTV (closed circuit TV) - закрытая система видеонаблюдения, имеет в своем составе как минимум одну камеру и монитор для наблюдения. Для записи событий может применяться цифровой видео рекордер (DVR). Доступ к видеоинформации могут иметь только пользователи, которые непосредственно подключены к этой системе. IPTV (Internet Protocol Television) в отличие от CCTV, камеры подключаются к IP сети (интернет) что позволяет системе контролироваться и управляться через интернет, из любой точки мира, используя любой стандартный браузер. Данные видеонаблюдения также могут легко сохраняться, используя сетевой видео рекордер (NVR).

предотвращаются камерами. Вообще говоря, технология очень слабо влияет на снижение числа «спонтанных» преступлений.

- *Основное влияние этой технологии на поведение людей касается больше общественного порядка, чем противоправных действий. Практически большинство систем видеонаблюдения борются с «антисоциальным поведением», включая тех, кто оставляет мусор, справляет малую нужду в парках, а также малолетних курильшиков, нарушение правил дорожного движения, надписи на стенах, драки, обструкцию, пьянство, непристойное поведение и обман счетчиков на парковках. Конечно, найдутся аргументы, что именно на эти цели ориентирована данная технология, но слишком малая часть общественности ассоциирует системы CCTV с такими проступками.*
- *Данной технологии присущ целый ряд отрицательных моментов, о которых не сообщается. Я лично могу засвидетельствовать, что операторы постоянно дискриминируют людей из-за своих личных предубеждений по расовой принадлежности, возрасту, классовой принадлежности и сексуальным предпочтениям. Результаты проведенного недавно исследования подтверждают эту точку зрения. Несколько случаев неправильного использования этой технологии и полученных изображений внесли свой вклад в склонение общественного мнения к поддержке технологии. Системы CCTV являются также ключевым фактором, вызвавшим целый ряд изменений в деятельности полиции. Эти изменения, включая смещение практики с упреждающей на реагирующую, еще не были адекватно изучены и оценены»[1].*

Мы оставляем огромные массивы персональной информации онлайн. Ежедневно через почтовые серверы проходят миллиарды электронных писем. В сети «Facebook» хранятся более сотни мегабайт персональных фотографий и видео на каждого пользователя. Через платежные системы проходят сотни миллиардов персонально помеченных финансовых платежей. Большинство совершеннолетнего населения в развитых странах постоянно транслирует свои текущие координаты через мобильные сети.

> Каждый раз, когда вы снимаете деньги в банкомате, компьютер записывает не просто количество снятых денег, но сам факт вашего нахождения в конкретном месте в конкретное время. Попутешествуйте в интернете, и веб-сервер не просто отметит, какие страницы вы просмотрели, но и скорость вашего модема, тип использованного браузера и даже ваше географическое местоположение. В нашем обществе превалируют компьютеризованные системы записи и хранения информации, и мы вскоре будем наблюдать все большее число случаев, когда информация, собираемая такими системами для одной цели, будет использована совсем для другой. Развитие современных технологий делает этот сценарий все более реалистичным. Раньше компьютеры просто не могли хранить всю доступную им информацию: системы проектировались так, чтобы периодически стирать данные, которые им больше не нужны. Но современный уровень развития технологий хранения информации позволяет хранить данные практически бесконечно, после того, как они перестали быть нужными для той цели, с которой собирались. В результате сегодня в сети можно получить практически

1 Clive Norris and Garry Armstrong, «The Unforgiving Eye: CCTV Surveillance in Public Space», Centre for Criminology and Criminal Justice, University of Hull, Hull HU6 7RX, U.K. Цитируется по «Prejudice Drives CCTV Targets», KDIS Online, 24 октября 1997. http://merlin.legend.org.uk/~brs/archive/stories97/Suspects.html; Simon Davies, «Summary of Oral Evidence of Simon Davies», 23 октября 1997. Доступно в Интернете по адресу http://www.privacy.org/ pi/issues/cctv/lords_testimony.html.

полное досье на каждого из нас, поскольку почти каждое действие в интернете может быть использовано для идентификации и профилирования [1].

С развитием технологий «больших данных» (Big Data) угрозы усиливаются, поскольку объединяться может не только информация, содержащаяся в базах, данных, но и видео-, аудиоинформацию, наши следы в интернете и пр. В эпоху больших данных, облачных вычислений, систематического массового слежения насущной необходимостью становится возможность контролировать свою «информационную тень».

Современные системы анализа больших массивов данных (Big Data) позволяют установить уникальный профиль человека даже без слежки, а просто путем анализа его перемещений по координатам GSM-телефона и изображению с общедоступных камер наружного наблюдения, а также с помощью анализа интернет-трафика. Сохранить анонимность при генерации столь огромного массива информации становится практически невозможно.

Почти каждое действие в интернете может быть использовано для идентификации и профилирования. Современные системы анализа больших массивов данных (Big Data) позволяют установить уникальный профиль человека даже без слежки, а просто путем анализа его перемещений по координатам GSM-телефона и изображению с общедоступных камер наружного наблюдения, а также с помощью анализа интернет-трафика. Сохранить анонимность при генерации столь огромного массива информации становится практически невозможно.

Рекомендация Комитета министров Совета Европы CM (2010) 147 «О защите индивидов при автоматической обработке персональных данных в контексте профилирования». Извлечения

Информационные и коммуникационные технологии (ИКТ) делают возможными сбор и обработку больших объёмов данных, включая персональные данные, как в частном, так и в общественном секторах; отмечая, что данные ИКТ используются в большом диапазоне различных целей, в том числе для использования услуг, общепринятых и ценных для общества, потребителей и экономики; отмечая в то же время, что беспрерывное развитие конвергентных технологий создает для общества новые вызовы в связи со сбором и дальнейшей обработкой данных. Такие сбор и обработка информации могут проводиться в различных ситуациях и для достижения различных целей, и касаются различных видов данных, таких как информационные потоки, запросы пользователей интернета, привычки потребителя, их деятельность, образ жизни и поведение пользователей телекоммуникационных устройств, в том числе данные о месте (местах) их нахождения, а также данные, получаемые, в частности, из социальных сетей, систем видеонаблюдения, биометрических систем и радиочастотной идентификации (РЧИД), предвестников «интернета вещей», а также, отмечая желательность оценки различных ситуаций и целей в дифференцированной и многообразной форме.

В результате этого установления связей между большим количеством персональных, пусть даже анонимных заключений, метод профилирования граждан может отразиться на соответствующих людях, поскольку они попадают в определенные категории, причем зачастую об этом не зная. Профильные характеристики, когда они присваиваются субъекту данных, делают возможным создание новых персональных данных, которые не являются идентичными тем, которые были переданы указанным субъектом контролеру или которые известны контролеру, как могли обоснованно полагать лица, передающие эти данные. Не-

1 Гарфинкель, С. (2003) Все под контролем: Кто и как следит за тобой. Доступно через: http://www.uhlib.ru/kompyutery_i_internet/vse_pod_kontrolem_kto_i_kak_sledit_za_toboi/index.php.

достаточная прозрачность или даже просто «невидимость» профилирования граждан и отсутствие точности, которая может проистекать из автоматического применения заранее установленных правил для выводов, может создавать значительный риск для прав и свобод человека[1].

Пользователи предоставляют крупным компаниям колоссальные объемы данных о своей повседневной жизни, в том числе и конфиденциальной, и считают, что компании будут осторожно обращаться с нашими данными, однако гарантия есть не всегда. Когда же на основе этой информации принимаются неполезные для нас решения, о них обычно не сообщается[2].

Существуют специализированные компании, которые собирают общедоступные данные и привязывают их к профилям конкретных людей, с указанием имени, адреса и т.д. Например, американская компания «Acxiom» уже накопила базу данных по 1500 классификаторам на 500 миллионов пользователей со всего мира. Компания заявляет, что по составленным профилям может прогнозировать реакцию потребителей на различные раздражители (товары, бренды и проч.) [3]. Такие компании способны даже автоматически предсказывать местонахождение пользователей, анализируя архивные GPS-метки. По последним экспериментальным данным точность составляет 80% в течение 80 недель[4].

Вы просыпаетесь от телефонного звонка. Не может быть?! Несколько месяцев назад вы запрограммировали свой телефон таким образом, чтобы он не пропускал входящие звонки до 8 утра, однако на часах всего лишь 6:45. Кто может звонить в такое время? И самое главное, кто смог обойти блокировку звонков?

Вы снимаете трубку и тут же бросаете ее обратно – вас разбудила машина, проигрывающая рекламные сообщения. Реклама при помощи производимых компьютером телефонных звонков была запрещена в Соединенных Штатах Америки более десяти лет назад, но после того, как стоимость международных звонков упала ниже 10 центов за минуту, их поток хлынул в Северную Америку со всего мира. Причем почти все они – рекламные, вследствие большой популярности программируемых телефонных аппаратов. Но вас беспокоит еще одна проблема: как звонок прошел через установленный фильтр? Причину вы узнаете несколько позже: производитель купленного вами телефонного аппарата предусмотрел в его конструкции «черный ход», информация о котором отсутствует в документации. Зато информация о секретных кодах, позволяющих обойти защиту, продавалась неделю назад на онлайн-аукционе. Вы не обратили на это внимания и потеряли свой шанс выкупить свои спокойствие и неприкосновенность. М-да...

Раз уж вы проснулись, вы решаете разобрать вчерашнюю почту. В ней обнаруживается письмо из ближайшей больницы. «Мы очень рады, что травматологическое отделение нашей больницы смогло оказать Вам необходимую помощь в нужный момент», – начинается письмо. «Как Вам известно, плата, которую мы берем в соответствии с Вашей медицинской страховкой не покрывает наших расходов. Чтобы покрыть эту разницу многие больницы начинают продавать информацию о своих пациентах фирмам, занимающимся медицинскими исследованиями и изучением потребительского спроса. Вместо того чтобы следовать

1 Council of Europe Recommendation of the Committee of Ministers (2010) CM(2010)147 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling. Доступно через: https://wcd.coe.int/ViewDoc.jsp?id=1693029 Русский текст http://cyberpeace.org.ua/files/iii_6.pdf.

2 Паризер, Э. (2012) за стеной фильтров. Что интернет скрывает от нас . Москва, Альпина.

3 Tucker, P. (2013) Has Big Data Made Anonymity Impossible?. Доступно через: http://www.technologyreview.com/news/514351/has-big-data-made-anonymity-impossible.

4 Sadilek, A., Krumm, J.(2012) Far Out: Predicting Long-Term Human Mobility. Доступно через: http://www.cs.rochester.edu/~sadilek/publications/Sadilek-Krumm_Far-Out_AAAI-12.pdf.

этой порочной практике, мы решили обратиться к Вам с просьбой помочь нам компенсировать разницу. Рекомендуемый размер пожертвования – 275 долларов – компенсирует стоимость Вашего обращения к нам. На эту же сумму будет уменьшен размер уплачиваемых Вами налогов».

Вы осознаете, что этот маленький шантаж не пустые слова, но не находите ничего особо страшного в том, что кто-то узнает о растяжении связок на вашем запястье. Вы сгибаете лист пополам и отправляете его в машинку для уничтожения бумаг в компании троицы малоинтересных предложений по кредитным картам.

Почему именно в машинку, а не просто в корзину? Еще несколько лет назад вам бы и в голову не пришло уничтожать бумажки с рекламными предложениями, пока с одним из ваших друзей не произошел неприятный инцидент: его личность «временно украли». Служащий жилого комплекса извлек из мусора полученные на имя вашего друга предложения по открытию кредитных карт, позвонил по указанному там бесплатному телефонному номеру, и ему доставили кредитные карточки. Сейчас он в Мехико, вместе с кучей дорогих вещей и электроники, приобретенных за счет вашего друга. На этой радостной ноте вы берете свой портфель и направляетесь к двери, которая автоматически закрывается за вашей спиной.

Когда вы входите в лифт, скрытая видеокамера сканирует ваше лицо, автоматика идентифицирует личность и направляет лифт в подземный гараж. Попутчиков в лифте лучше избежать, ибо у вас нет желания повторить ситуацию, которая случилась на прошлой неделе с беднягой в доме 4G. Оказалось, что его соседка рассталась недавно со своим дружком буйного нрава и ему было запрещено приближаться к ней. Естественно, лифт был запрограммирован на опознание этого человека, и, когда он вошел в лифт, двери были заблокированы до приезда полиции. К несчастью, в этот момент в лифте находились и другие люди. Никто не мог предположить, что буйный нрав нарушителя не единственная его проблема, ко всему прочему он страдал не диагностированной вовремя клаустрофобией. Ситуация с захватом заложников развивалась очень быстро, но закончилась слишком плохо для мистера 4G. К счастью, все было записано на видеопленку.

Бортовой компьютер вашего автомобиля посоветовал три варианта маршрута поездки на работу сегодня утром. Вы выбрали не очень удачный и провели в автомобильных пробках более получаса. Во время вынужденного простоя компьютер каждые пять минут проигрывал рекламу булочек с начинкой, однако вы не могли его выключить: компьютер бесплатный и окупается за счет рекламы.

Ваше опоздание на работу не осталось не замеченным для корпоративной системы учета рабочего времени. В полученном от нее по электронной почте сообщении вам предлагалось несколько вариантов компенсации времени опоздания: не ходить сегодня на обед, задержаться на 45 минут вечером или вычесть это время из и так уже истощившегося отпуска. Выбор за вами. Вы оглядываетесь по сторонам и выдавливаете на лице улыбку. Маленькая видеокамера на мониторе вашего компьютера транслирует изображение вашей улыбки боссу и коллегам. Считается, что Workplace Video Wallpaper™ способствует формированию духа товарищества, но компания-производитель этого программного обеспечения утверждает также, что постоянный мониторинг сокращает количество конфликтов на рабочем месте, предотвращает флирт и даже употребление наркотиков. Теперь на рабочих местах все улыбаются: не делать этого опасно.

Видеокамера лишь один из механизмов непрерывного мониторинга на работе. На книгах и журналах установлены электронные метки, призванные остановить постоянные хищения из библиотеки компании. После паники, случившейся в результате сообщения о бомбе, все служащие обязаны постоянно носить иден-

тифицирующие таблички, а столы и шкафчики подвергаются периодическому досмотру. (Ходят слухи, что начальник службы безопасности сама организовала звонок с сообщением о бомбе, чтобы получить повод для введения новых порядков.)

В следующем месяце компания планирует установить в умывальных комнатах специальные устройства, которые будут следить, чтобы служащие мыли руки. Хотя первоначально эти устройства были разработаны для учреждений здравоохранения и пищевой промышленности, последние исследования показали, что регулярное мытье рук снижает распространение заболеваний среди офисных работников. Так что машины будут установлены, и с этого момента вы потеряете еще немного своей приватности и достоинства[1].

Однако данные, на основании которых можно идентифицировать индивида, собираются не только правительствами и коммерческими компаниями. Пользователи различных ресурсов и сервисов глобальной сети интернет – *это сотни тысяч «маленьких братьев»*, которые поставляют видео-, аудио- и текстовую информацию о людях онлайн.

В фантастическом романе «Лавина» американский писатель Нил Стивенсон изобразил людей - «горгулий», которые записывали все, что видели вокруг, и загружали эту информацию в огромный банк данных Центральной разведывательной корпорации, рассчитывая, что она кому-нибудь понадобится и за нее заплатят. В 1980-х гг. Стив Манн начал носить видеокамеру на голове. Камера была присоединена к радиопередатчику, посылавшему изображение на веб-сервер, где картинка отображалась под заголовком «Посмотрите, что я вижу сквозь мои очки прямо сейчас (или во время последней передачи)». Кроме того, он поместил на шляпу карточку с предупреждением: «Для вашей защиты видеозапись Вас и Вашего окружения может быть передана и сохранена в удаленном месте. Все преступные действия не останутся безнаказанными!!!»[2]. Сегодня обладатели очков «Google glasses» имеют возможность фиксировать и транслировать онлайн все, что они видят, не задумываясь о том, в какой степени это может нарушать право других «оставаться в одиночестве».

Превращение персональной информации в товар – еще одна угроза информационному самоопределению личности. «Идентифицирующая личность информация: имя, профессия, хобби и другие мелочи, делающие человека уникальным, превращается в объект владения, - пишет Э. Паризер. - Но владеют этим объектом не конкретные индивидуумы, контролирующие информацию о себе, а крупный бизнес, постоянно использующий его для получения прибыли и захвата рынка. Как можно ощущать собственную ценность, не владея в полной мере даже собственным именем?»[3]

Еще одна опасность – *это персонализация потоков сообщений*, которая лишает человека возможности контролировать информацию, которую он получает.

Код, лежащий в основе персонализации, довольно прост, поясняет Э. Паризер: «Фильтры нового поколения изучают то, что вам, судя по всему, нравится: ваши предшествующие действия или то, что нравится людям, похожим на вас, — и пытаются экстраполировать эти данные. Это механизмы предсказаний, постоянно уточняющие теорию о том, кто же вы на самом деле, что вы сделаете и чего захотите дальше. Вместе они творят уникальную информационную вселенную для каждого из нас — я называю этот процесс возведением «стены фильтров» — и фундаменталь-

1 Гарфинкель, С. (2003) Все под контролем: Кто и как следит за тобой. Доступно через: http://www.uhlib.ru/kompyutery_i_internet/vse_pod_kontrolem_kto_i_kak_sledit_za_toboi/index.php.

2 Там же.

3 Паризер, Э. (2012) за стеной фильтров. Что интернет скрывает от нас. Москва, Альпина.

но меняют наш подход к восприятию информации»[1]. Тем самым стирается граница между удобством сервиса и вмешательством – контролем поведения и непосредственным влиянием на личность.

Стена фильтров невидима, предупреждает Э. Паризер, а задачи инструментов персонализации непрозрачны: сервис не говорит вам, за кого вас принимает или почему показывает конкретные ссылки. Вы не знаете, правильны ли его предположения о вас или нет, и, возможно, вы даже не в курсе, что он делает такие предположения. В итоге вы оказываетесь за стеной не по собственному желанию: персонализированные адаптационные интернет-фильтры вмешиваются в вашу жизнь, и, поскольку они приносят прибыль сайтам, на которых установлены, их все труднее избегать[2].

Демократизация деструктивных технологий, информационные войны, создающие угрозу национальной безопасности, побуждают правительства все в большей степени использовать системы массированного систематического наблюдения. События последних лет показали, насколько опасной для сохранения неприкосновенности частной жизни может быть такая деятельность при отсутствии надлежащих инструментов регулирования.

Непосредственную угрозу информационной приватности представляют *различные виды компьютерных преступлений*. Большинство из них – это «старые» нарушения неприкосновенности частной жизни, совершенные с использованием информационно- коммуникационных технологий. Некоторые же, например, кража личности - это совершенно новая опасность.

Кража идентичности. Случай Стивена Шоу.

В один прекрасный летний день 1991 года продавец автомобилей из Орландо, штат Флорида, Стивен Шоу, получил доступ к кредитному отчету журналиста Стивена Шоу. Сделать это было проще простого. В течение многих лет компания «Equifax» вела агрессивную рекламную кампанию своих услуг по предоставлению кредитных отчетов фирмам, торгующим автомобилями. Услуга предоставляла продавцу возможность, узнав имя потенциального покупателя, ненадолго отлучиться и быстро произвести проверку его кредитной благонадежности. Вероятнее всего, мистер Шоу из Флориды использовал эту возможность, чтобы «вычислить» кого-нибудь с созвучным именем и незапятнанной кредитной историей, считает Стивен Шоу. Как только Стивен Шоу из Флориды узнал номер социального страхования и другую личную информацию Стивена Шоу из Вашингтона, он получил возможность «украсть личность» последнего. Помимо сведений о безупречной кредитной репутации Стивена Шоу, его кредитный отчет содержал настоящий и предыдущие адреса места жительства, девичью фамилию матери и номера всех его кредитных карт. «Он воспользовался моими данными для открытия 35 счетов и нанес мне ущерб в размере 100 000 долларов, – рассказывал Стивен Шоу. –повсюду брал кредиты на покупку автомобиля, персональные кредиты, открывал банковские счета, покупал дорогую стереоаппаратуру, мебель, домашнюю технику, вещи, авиабилеты».

Поскольку все счета были открыты на имя Стивена Шоу с использованием его номера социального страхования, ему автоматически предъявлялись к оплате все траты, которые на самом деле производил другой Шоу – из Флориды. Коль скоро счета не оплачивались, пострадавшие фирмы сообщили компании

1 Там же.
2 Там же.

«Equifax» и другим кредитным бюро, что Стивен Шоу, имевший ранее безупречную кредитную репутацию, стал теперь неблагонадежным[1].

Эта далеко не исчерпывающая характеристика угроз неприкосновенности частной жизни, возникающих в процессе сбора, обработки и хранения персональных данных в различных контекстах, с очевидностью доказывает необходимость разработки эффективных мер их защиты.

1 Гарфинкель, С. (2003) Все под контролем: Кто и как следит за тобой. Доступно через: http://www.uhlib.ru/kompyutery_i_internet/vse_pod_kontrolem_kto_i_kak_sledit_za_toboi/index.php.

Раздел 2.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ КАК ПРОБЛЕМА ПУБЛИЧНОЙ ПОЛИТИКИ



ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ КАК ПРОБЛЕМА ПУБЛИЧНОЙ ПОЛИТИКИ: ИСТОРИЯ

Хотя примеры сбора данных об индивидах можно найти и в античности, и в средневековье, современная система государственного учета стала формироваться с укреплением бюрократического государства. Институционализация сбора сведений об индивидах – общий процесс, характерный для всех стран. Современные информационно-коммуникационные технологии позволяют собирать беспрецедентные объемы данных об индивидах.

Хотя примеры сбора данных об индивидах можно найти и в античности, и в средневековье, современная система государственного учета стала формироваться с укреплением современного бюрократического государства. Расширение и укрепление государственной власти требовало сложной системы учета, в том числе и данных об индивидах[1]. Традиционно можно говорить о трех типах информации об индивидах:

- *административные данные (взаимодействие с государственными органами, используемые для регулирования, выдачи разрешений (лицензирования), рассмотрения различных вопросов – обращений за помощью, отчеты о доходах, брачные свидетельства и т.п.);*
- *разведывательные и полицейские данные;*
- *исследовательские и статистические данные (общие отчеты о состоянии дел, планирование, переписи населения и пр.)*[2].

Институционализация сбора сведений об индивидах – процесс, характерный для всех современных государств. Новые информационно-коммуникационные технологии позволили собирать беспрецедентные объемы данных об индивидах, вследствие чего политика в отношении сбора, обработки и защиты персональных данных стала одной из важных проблем государственного управления.

> *Необходимость защиты информационной приватности была очевидна уже в конце XIX в. В 1948 г право на неприкосновенность частной жизни было включено в Международный пакт о гражданских и политических правах. С середины 1960-х гг. вопросы о том, как обрабатывается и хранится информация, собираемая о гражданах государственными органами и частными компаниями, привлекали внимание общественности*

В 1948 г. защита неприкосновенности частной жизни вошла в Международный пакт о гражданских и политических правах (ст. 17)

1 Tilly, Ch. (1975) The Formation of National States in Western Europe. Princeton, N.J.: Princeton University Press; Dandeker, Ch. (1990) Surveillance, Power, and Modernity: Bureaucracy and Discipline from 1700 to the Present Day/ St. Martin's Press.

2 Westin, A. Baker, M. (1972) Databanks in a Free Society: Computers, Record-Keeping and Privacy. Quadrangle Books.

«Никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств. Из этого базового неотчуждаемого права на неприкосновенность личной жизни вытекает право индивида на защиту персональных данных».

Однако общественность в разных странах достаточно индифферентно относилась к информации, собираемой государством и даже к тому, что определеные решения принимались на основании этой информации. Хотя в этот период активно развивалось движение за гражданские права, активисты и общественные организации обращали мало внимания на информационную приватность. Проблема защиты данных была хорошо определена, но не обсуждалось какое-либо специальное законодательство.

К середине 1960-х годов, в связи с созданием централизованных правительственных банков, необходимость исключения возможностей несанкционированного доступа к информации стала очевидной не только специалистам коммерческих предприятий и государственных организаций, но и гражданам. В целом ряде стран Европы и в США были созданы комиссии и исследовательские группы для изучения природы, динамики и влияния технологий на неприкосновенность частной жизни, а также способов обеспечения приватности в новых условиях.

Вашингтон, федеральный округ Колумбия, 1965 год. Предложение Бюджетного бюро было столь же простым, сколь и революционным. Вместо того чтобы выделять каждому ведомству средства на приобретение компьютеров, создание технологий хранения данных, зарплату обслуживающего эту инфраструктуру персонала, правительству Соединенных Штатов Америки предлагалось сформировать Национальный информационный центр. Проект должен был начаться с объединения информации из различных ведомств: данных о населении и его размещении из Бюро переписи населения; данных о трудоустройстве из Бюро трудовой статистики; данных о налогах и сборах из Налогового управления и информации о выплатах из Управления социального страхования. В дальнейшем предполагалось хранить и другую информацию. Несмотря на то что изначальная цель заключалась в простом снижении издержек, очень скоро стало ясно, что проект таит в себе и другие выгоды. Из общенационального массива данных можно легко и точно получать статистическую информацию. Создание единой общенациональной базы данных позволяет избежать трудностей, возникающих из-за неправильного написания имен, и других проблем, характерных для крупных банков данных. Единая база данных также позволяет правительству (и не только ему!) использовать накопленную информацию самым эффективным образом.

Принстонский институт перспективных исследований опубликовал отчет, с энтузиазмом поддерживающий проект создания базы данных, в котором говорилось, что централизованное хранение информации обеспечит более высокий уровень ее безопасности и таким образом лучше обеспечит приватность в национальном масштабе. Карл Кайзен, директор института и руководитель исследовательской группы, утверждал также, что конгресс примет необходимые законодательные акты, которые обеспечат дополнительную защиту информации в базе, гарантируют ее приватность и обеспечат подконтрольность обслуживающего базу персонала. Зацикливание на идее привело к тому, что концепция Национального информационного центра переросла в желание создать огромный банк данных, содержащий самую подробную информацию о каждом гражданине США от момента рождения и до смерти. В базе данных должны были храниться: электронное свидетельство о рождении каждого гражданина, сви-

детельство о гражданстве, школьные оценки, данные о воинской обязанности и прохождении военной службы, записи о налогах, социальных выплатах, информация о владении недвижимостью и, конечно, запись о смерти. ФБР могло бы даже использовать систему для хранения информации о преступлениях.

Рекламирующая проект статья появилась в издании «Saturday Review» 23 июля 1966 года. Заголовок объяснял все: «Автоматизированное правительство: Как компьютеры будут использоваться Вашингтоном для упрощения управления человеческими ресурсами на благо каждого». Но статья не достигла своей цели. Вместо восторженной поддержки технократического подхода конгресс США инициировал серию слушаний по проблеме угроз, возникающих при использовании компьютерных банков данных. Шесть месяцев спустя журнал «New York Times Magazine» опубликовал статью под заголовком «Не говори об этом компьютеру», злобно атаковавшую правительственную идею централизованного накопления информации. Написанная Вэнсом Паккардом, автором «Обнаженного общества» (бестселлер, описывающий, как правительство, бизнес и образовательные учреждения вторгаются в личную жизнь), публикация в «Times» акцентировала внимание на ключевом аргументе против проекта: «Самой страшной опасностью централизованного накопления информации в компьютерных базах данных является сосредоточение огромной власти в руках людей, управляющих этими компьютерами. Когда все детали нашей жизни будут помещены в центральный компьютер или другую глобальную систему хранения информации, мы все в некоторой степени попадем в зависимость от людей, контролирующих эти машины».

Уже в 1968 году Бюджетное бюро заявило, что сомневается в том, что план практической реализации центра будет представлен на рассмотрение конгрессу. Тем временем специальный подкомитет Палаты представителей по защите неприкосновенности частной жизни выпустил отчет, в котором говорилось, что обеспечение приватности должно стоять на одном из первых мест при разработке проектов компьютерных банков данных, работы по созданию Национального информационного центра должны быть приостановлены до тех пор, пока проект не сможет гарантировать приватность, а Бюджетное бюро совершило ошибку, не разработав предварительно процедуры обеспечения приватности.

Национальный информационный центр так и не был создан. Вместо этого каждое ведомство продолжало развивать свои собственные компьютерные системы. Взамен создания единого банка данных, который мог быть использован не слишком стесняющимся в выборе средств бюрократическим аппаратом для осуществления незаконного контроля над судьбами отдельных людей, правительство учредило десятки банков данных[1].

В 1967 г. было опубликовано первое фундаментальное исследование – монография профессора права Колумбийского университета (США) А. Уэстина «Приватность и свобода», в которой он анализировал последствия распространения автоматизированной обработки данных и призывал к разработке новых стандартов приватности и новых действий в отношении защиты приватности[2]. Обозначая угрозы неприкосновенности частной жизни, А. Уэстин ввел понятие «электронной тени» - «километров» цифровых записей о людях, хранящихся в разнообразных автоматизированных системах.

В марте 1968 г. Алан Уэстин выступил с показаниями перед специальным подкомитетом конгресса по защите неприкосновенности частной жизни относительно угрозы этой гражданской свободе, исходящей от кредитных бюро. Выступление

1 Гарфинкель, С. (2003) Все под контролем: Кто и как следит за тобой. Доступно через: http://www.uhlib.ru/kompyutery_i_internet/vse_pod_kontrolem_kto_i_kak_sledit_za_toboi/index.php.
2 Westin, A. (1967) Privacy and Freedom. New York: Atheneum.

Уэстина имело ключевое влияние на принятие конгрессом закона «О точной отчетности по кредитам». Оно также убедило советника президента Э. Ричардсона в необходимости создания Консультативного комитета по автоматизированным системам обработки персональной информации. В 1972 г. возглавляемая Ричардсоном комиссия опубликовала Кодекс добросовестного использования информации - один из первых в мире документов, определяющих принципы защиты персональной информации[1].

Ответом на возникшие проблемы стали:

- *разработка и внедрение технических решений по защите информации;*
- *разработка мер правовой регламентации деятельности, связанной со сбором, обработкой, хранением и распространением информации.*

В 1970-х годах из всего объема обрабатываемой информации была выделена особая группа сведений, касающихся частной жизни конкретных людей, которые собирались, обрабатывались, хранились и распространялись различными организациями, службами и частными лицами. Эти сведения получили название «информация о личности», «данные о физических лицах» или «персональные данные»[2].

Впервые проблема законодательной защиты персональных данных была сформулирована в США. В 1966 г. сенатор Джон Мак Карти предложил «Билль об ЭВМ и о правах», послуживший основой Правил о секретности. В соответствии с этим документом каждому гражданину должно было быть предоставлено право знать содержание файла, которое его касается. В правилах также предлагалась простая процедура для исправления возможных ошибок сведений.

К началу 1970-х гг. акцент сместился с технического и юридического регулирования в сторону защиты гражданских прав. Это изменение нашло отражение в новых законах, признававших права физического лица вмешиваться в сам процесс обработки данных.

С интенсификацией потоков данных и их обработки в рамках международного сотрудничества, экономического взаимодействия и торговли стала актуальной проблема трансграничной передачи данных. ООН, ОЭСР, Совет Европы стали основными форумами для поиска ответов на новые вызовы[3].

В 1980-е гг. проблема защиты персональных данных приобретает самостоятельность по отношению к обеспечению неприкосновенности частной жизни в целом.

В 1980-е гг. с технологической точки зрения, несмотря на развитие распределенных компьютерных сетей и персональных компьютеров, существенных изменений в отношении угроз приватности не произошло.

Однако, с распространением практик сбора и обработки сведений о гражданах коммерческими компаниями и правительственными органами проблема защиты персональных данных приобретает самостоятельность по отношению к обеспечению неприкосновенности частной жизни в целом. Хотя граждане все с большей настороженностью относились к объединению банков данных различных правительственных организаций или коммерческих предприятий, с политической точки зрения информационная приватность оставалась второстепенной проблемой. Тем

1 Гарфинкель, С. (2003) Все под контролем: Кто и как следит за тобой. Доступно через: http://www.uhlib.ru/kompyutery_i_internet/vse_pod_kontrolem_kto_i_kak_sledit_za_toboi/index.php.
2 Иванский, В.Op.cit.
3 United Nations university, human rights and scientific and technological development (1990) Доступно через: http://archive.unu.edu/unupress/unupbooks/uu06he/uu06he00.htm#Contents.

не менее, в этот период были разработаны ключевые международные документы, устанавливающие основания и процедуры защиты персональных данных.

Организация экономического сотрудничества и развития (ОЭСР) стала первой международной структурой, занявшейся проблемой защиты персональных данных. Руководство по защите персональных данных, разработанное ОЭСР в 1980 г., до сих пор является основным документом, постулирующим нормы политики в отношении персональных данных[1].

В это же время Совет Европы готовил документ в сфере защиты персональных данных. Экспертная группа ОЭСР поддерживала тесные контакты с Советом Европы для того, чтобы избежать ненужных расхождений. Через несколько месяцев после руководства ОЭСР, в начале 1981 г. Совет Европы опубликовал Конвенцию о защите персональных данных, подвергающихся автоматической обработке[2].

Конвенция до сих пор является единственным международным юридически обязывающим документом: все подписавшие ее страны должны выполнить требования конвенции. Конвенция включила принципы добросовестной работы с информацией и ряд прав защиты индивидуумов (право на информацию, доступ и исправление ошибок). В отношении международного регулирования Конвенция предусматривала создание специализированных учреждений и инструментов. Однако по сути Конвенция предлагала создание двухсторонних, а не международных механизмов. Кроме того, в Конвенции впервые было зафиксировано формальное требование адекватности мер защиты для обмена персональными данными между странами (ст. 12). Благодаря этому принципу национальные законы о защите персональных данных в большинстве случаев учитывали положения Конвенции.

ООН обратилась к сфере приватности данных и, в частности, к компьютеризированным персональным файлам в 1980 г.[3] Работа началась в подкомиссии по вопросам дискриминации и меньшинств Верховного комиссара по правам человека. Первый набор принципов был разработан в 1983 г., но работа шла крайне медленно. Почти десятилетии потребовалось ООН для того, чтобы подготовить собственное руководство по защите приватности данных, которое было опубликовано в 1990 г.[4].

- *Документы ОЭСР*

  Организация экономического сотрудничества и развития в 1980 г. приняла Руководящие принципы ОЭСР в области неприкосновенности личной жизни. В 1985 году за ними последовала Декларация о трансграничных потоках данных. В 2013 году была принята обновленная редакция Руководящих принципов.

- *Конвенция Совета Европы (1981)*

Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера (108-я конвенция) - первый обязательный для исполнения международный правовой договор о неприкосновенности личной жизни. В нем определен ряд главных принципов, в дальнейшем положенных в основу многих законов о неприкосновенности личной жизни. Конвенция также защищает физических лиц от вторжения в их личную жизнь со стороны государственных органов и администрации частных организаций. Ратификация конвенции осуществляется в

1 Hert, P. (2013) Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency? Доступно через: http://moritzlaw.osu.edu/students/groups/is/files/2013/08/7-Hert-Papakonstantinou.pdf.

2 Совет Европы (1981) Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера Страсбург, 28 января 1981 года. Доступно через: http://conventions.coe.int/treaty/rus/Treaties/Html/108.htm.

3 Там же.

4 Руководящие принципы регламентации компьютеризированных картотек, содержащих данные личного характера, приняты резолюцией 45/95 Генеральной Ассамблеи от 14 декабря 1990 года. Доступно через: http://www1.umn.edu/humanrts/instree/Rq2grcpd.html.

добровольном порядке, однако для стран, ее подписавших, она является юридически обязательным документом. На сегодняшний день конвенция ратифицирована 47 странами. Она открыта для подписания странами, как являющимися членами Совета Европы, так и другими государствами и даже международными организациями. Этим правом воспользовалась и Европейская комиссия, присоединившаяся к Конвенции как самостоятельный субъект международного права.

Принципы ОЭСР и Конвенция Совета Европы относятся к первому поколению документов о защите персональных данных[1]. Национальные стратегии в области защиты персональных данных, принятые в этот период, базировались именно на принципах этих документов и потому также относятся к первому поколению документов.

Существенные изменения технологий произошли в 1990-х гг. (WWW, мобильные средства коммуникации, биометрия), что повлекло принципиальные изменения практик управления (систем государственного учета, национальной безопасности, борьбы с преступностью). Поскольку сбор, хранение и обработка персональных данных – одна из основ транснационального интернет-бизнеса, активный интерес к разработке политики в отношении защиты персональных данных стали проявлять коммерческие структуры. Актуализировалась и деятельность на международном уровне.

> *Руководящие принципы ООН по регламентации компьютеризированных картотек, содержащих данные личного характера (1990 г.) требуют соблюдения следующих норм:* «юбое лицо, удостоверяющее свою личность, имеет право знать, подвергаются ли касающиеся его данные обработке, получать об этом сообщение в понятной форме, без излишних задержек и расходов, добиваться внесения соответствующих исправлений в данные или уничтожения их в случае их незаконной, необоснованной или неточной регистрации и, если эти данные сообщались кому–либо, знать их получателя. Следует предусмотреть возможность подачи, в случае необходимости, апелляции в контрольный орган» (ст. 8) Эти принципы относились только к автоматизированной обработке данных, включали принципы добросовестности и требовали создания независимого регулятора - уполномоченного органа (ст.9). Трансграничная передача данных была возможной только для стран с сопоставимыми или взаимно согласованными нормами (ст.9). Кроме того, в документе впервые обращалось внимание на защиту персональных данных в международных организациях. Руководящие принципы ООН также относятся к первому поколению документов о защите персональных данных.
>
> *Директива Европейского союза о защите данных 95/46/ЕС* была опубликована в 1995 г. Общие принципы, заложенные в директиву, аналогичны принципам Конвенции № 108 и Руководящим принципам ОЭСР.

Одним из первых примеров комплексной политики в отношении защиты персональных данных стал аналитический документ «Канадская информационная магистраль» (1994). Политика должна была включать:

- *разработку законодательства,*
- *разработку и внедрение добровольных стандартов приватности,*
- *продвижение технологий, обеспечивающих защиту персональных данных,*
- *просвещение граждан (пользователей)*[2].

1 Hert, P. (2013) Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency? Доступно через: http://moritzlaw.osu.edu/students/groups/is/files/2013/08/7-Hert-Papakonstantinou.pdf.

2 Raab, C, Hert, P. (2007) The Regulation of Technology: Policy Tools and Policy Actors. Tuburg University. Доступно через: http://tilburguniversity.nl/tilt/publications/workingpapers.

Проблема информационной приватности оказалась в центре внимания гражданских активистов. Именно в этот период неприкосновенность частной жизни онлайн, обеспечиваемая надлежащей защитой персональных данных, стала рассматриваться как необходимое условие осуществления гражданских прав и свобод.

К концу XX в. защита персональных данных была структурирована как политическая проблема и обеспечивалась на основе национальных стратегий и законов, международных соглашений, принципов, рекомендаций и деклараций.

Начало XXI в. ознаменовалось существенным изменением цифровой сферы частной жизни в связи с широким распространением технологий веб 2.0[1] (социальные поисковые системы, средства для сохранения закладок, социальные сервисы сохранения мультимедийных ресурсов, сетевые дневники (блоги), вики (wiki), социальные геосервисы и пр.), облачных вычислений и пр.:

- *технологии веб 2.0, позволяющие пользователям самостоятельно создавать контент, манипулировать им и управлять связями между своими и чужими материалами, привели к активизации коммуникации, координации и к включению пользователей не только в процесс использования и создания ресурсов, пополнение сервисов, но и в определение стратегии их развития;*
- *технологии облачных вычислений позволили увеличить мощности, доступные для хранения и обработки информации, как организациям (частным и государственным), так и индивидам. Однако с повсеместным приходом этой технологии возникла проблема создания неконтролируемых данных, когда информация, оставленная пользователем, хранится годами, часто без его ведома;*
- *технологии обработки больших объемов данных (Big Data) позволили анализировать и интегрировать данные, которые генерируются веб-сайтами, веб-журналами, видеозаписями, текстовыми документами, непространственными данными, сетями датчиков и иными источниками, но не соответствуют структурированному формату баз данных.*

Технологии Веб 3.0. В будущем более мощные системы смогут работать как персональные советчики в таких же неоднородных и сложных сферах, как финансовое планирование: например, составление пенсионного плана для семейной пары или образовательный консалтинг, когда тот или иной сервис выберет Вам оптимальный для поступления университет. Пример использования этой технологии – «KnowItAll», проект исследовательской группы Вашингтонского Университета, финансируемый «Google». В его рамках создана система «Opine», собирающая и сортирующая мнения пользователей с различных тематических сайтов. Демонстрационный проект, посвящённый отелям, «понимает» такие параметры, как температура в номере, комфортабельность кровати и цены, а также различает, что такое «великолепно», «неплохо» и «сойдёт», чтобы выдавать полезные ответы на запросы. На современных сайтах пользователю придётся просмотреть огромные списки комментариев и отзывов от других пользователей, а «вебтринольная» система будет сама взвешивать и ранжировать все комментарии, чтобы найти оптимальное, разумное решение и помочь рядовому пользователю быстро найти нужный отель.

«Это можно назвать Всемирной Базой Данных (World Wide Database)», – говорит Нова Спивак, основатель компании, разрабатывающей технологию, которая определяет отношения между кусочками информации в сети. – «Мы хотим пройти путь от интернета связанных документов к интернету связанной информации»[2].

1 О’Рейли, Т. (2005) Что такое Веб 2.0. Доступно через: http://old.computerra.ru/think/234100/.
2 Интернет здравого смысла (2006). Доступно через: http://habrahabr.ru/post/30866/.

Удлинившаяся «цифровая тень» стала заметнее для пользователей, что вызвало активные дискуссии о возможных угрозах информационной приватности и способах предотвратить эти угрозы. Результатом стали многочисленные инициативы на национальном, региональном и международном уровне[1].

Антитеррористические меры для обеспечения национальной безопасности, оказавшиеся в центре внимания правительств после событий 9 сентября 2001 г., и связанная с этим угроза массового систематического слежения и перехвата, оказавшаяся в центре общественного интереса после разоблачений Э. Сноудена в 2013 г., не оставили сомнения в том, что защита персональных данных стала серьезной и сложной проблемой публичной политики. Теперь уже не только гражданские активисты, но и правительства озаботились обеспечением приватности онлайн.

> В 2001 году к 108-й конвенции Совета Европы был принят Дополнительный протокол, который касается надзорных органов и трансграничных потоков данных. В нем содержится требование ко всем странам-членам СЕ предоставить надзорным органам полную независимость. Он также предусматривает учреждение национального надзорного органа, который обязан следить за соблюдением законодательства в области защиты данных и требовать от не присоединившихся к конвенции стран-получателей данных обеспечения адекватного уровня их защиты. Протокол дает право участникам конвенции принимать законодательные меры по ограничению потоков данных в не присоединившиеся к конвенции страны и ожидать аналогичного уровня защиты от страны-участника конвенции в отношении определенных категорий уязвимых данных.
>
> Директива ЕС о неприкосновенности личной жизни и об электронных коммуникациях 2002/58/ЕС установила конкретные требования, касающиеся сети интернет (сохранение данных, использование фрагментов данных типа cookies, а также включение личных данных в каталоги для общего пользования).
>
> В 2007 году, Совет ОЭСР принял новую Рекомендацию ОЭСР, касающуюся трансграничного сотрудничества в вопросе принудительного исполнения законов, охраняющих неприкосновенность личной жизни. Документ преследует цель оказания взаимопомощи при исполнении законов о неприкосновенности личной жизни. Ожидается, что он окажет влияние на взаимодействие на глобальном уровне.
>
> В 2009 году коалиция в составе более 100 различных групп подготовила Мадридскую декларацию о неприкосновенности личной жизни, в которой содержится призыв к установлению общемировых стандартов в области неприкосновенности личной жизни.
>
> В 2013 г. на Генеральной Ассамблее ООН была принята Резолюция «Право на неприкосновенность личной жизни в цифровой век», которая призывает «уважать и защищать право на неприкосновенность личной жизни, в том числе в контексте цифровой коммуникации», а также «принимать меры, с тем чтобы положить конец нарушениям этих прав и создавать условия для предотвращения таких нарушений, в том числе путем обеспечения того, чтобы касающееся этого национальное законодательство соответствовало их международным обязательствам по международному праву прав человека». В резолюции подчеркивается, «что незаконное или произвольное слежение за сообщениями и/или их перехват, а также незаконный или произвольный сбор личных данных, представляющие собой крайне интрузивные деяния, нарушают права на неприкосновенность личной жизни и свободу выражения мнений и могут идти вразрез с основополагающими принципами демократического общества».

1 International Principles on the Application of Human Rights to Communications Surveillance (2014). Доступно через: https://www.necessaryandproportionate.net/.

В настоящее время существует множество источников международных норм, политических принципов и инструментов как на глобальном, так и на региональном уровнях. Они в разной степени институционализированы и обладают различными полномочиями и компетенциями. Поскольку проблема разработки надлежащей политики в отношении защиты персональных данных до сих пор далека от разрешения, а по многим аспектам и слабо институционализирована, существенную роль в обсуждении принципов такой политики играют международные, региональные и национальные дискуссии на таких площадках, как Всемирный саммит ООН по вопросам информационного общества, Глобальный и региональные форумы по вопросам управления интернетом, конференции уполномоченных органов по защите персональных данных и пр.

> *В настоящее время существует множество источников международных норм, политических принципов и инструментов как на глобальном, так и на региональном уровнях. Они в разной степени институционализированы и обладают различными полномочиями и компетенциями. Поскольку проблема разработки надлежащей политики в отношении защиты персональных данных до сих пор далека от разрешения, существенную роль в обсуждении принципов такой политики играют международные, региональные и национальные дискуссии на таких площадках, как Всемирный саммит ООН по вопросам информационного общества, Глобальный и региональные форумы по вопросам управления интернетом, конференции уполномоченных органов по защите персональных данных и пр.*

ПРОБЛЕМЫ И АКТОРЫ

Суть защиты персональных данных как проблемы публичной политики заключается в необходимости должного обеспечение как качества и безопасности сбора, хранения и обработки данных, так и права индивида контролировать использование данных о себе.

На начальных этапах использования автоматизированных систем обработки данных о гражданах, проблема регулирования представлялась узко-юридической задачей: разработать регламент сбора, хранения и обработки таких данных, обязанности и права сторон и т.п.

Однако переход от «банков данных» к децентрализованным информационным системам, размывание различий между частным и государственным сектором (аутсорсинг, сбор данных) и распространение разнообразных технологий мониторинга и контроля потребовали разработки целого набора политических инструментов. Вместе с тем, стало очевидным, что проблема защиты персональных данных носит комплексный характер и при ее решении необходимо учитывать и *структурные факторы:* бюрократизацию организаций, глобализацию и развитие технологий

Защита персональных данных перестала быть проблемой, понимание которой доступно только технической элите и юристам, специализирующимся в сфере информационного права. Сейчас она обсуждается в правительстве и в корпорациях, на национальных и на глобальном уровнях, политиками, юристами и техническими специалистами, и общественными активистами.

Понятие «публичная политика» в самом общем виде трактуется как совокупность программ и приоритетов органов власти, механизмов и технологий реализации программ, выработанные на основе и с учетом ожиданий социальных групп (страт) их представителями; как систематические действия, которые осуществляет актор или группа акторов для решения общественно-значимых проблем.

Проблема входит в сферу публичной политики, если:

- *она социально значима,*
- *решение принимается правительством,*
- *в обществе существуют различные и даже взаимоисключающие позиции.*

В основе публичной политики в отношении персональных данных лежит рациональное убеждение в том, что политические принципы и нормы права могут обеспечить защиту от рисков, которые появляются с развитием новых технологий.

О социальной значимости проблемы защиты персональных данных и о том, как эта проблема оказалась в фокусе внимания национальных правительств и межправительственных организаций, шла речь в предыдущих разделах.

Дискуссии, как правило, касаются ответов на ключевые вопросы:

- *что именно должно защищаться,*
- *от чего необходима защита,*
- *каковы цели защиты,*
- *кто должен обеспечивать защиту,*
- *каковы инструменты защиты.*

В большинстве случаев обеспечение автономии индивида и контроля информации о себе признаются основными принципами политики в отношении персональных данных. Однако проблема баланса ценностей остаётся нерешённой.

Анализ международных и национальных дискуссий позволяет определить координаты формирования позиций следующим образом:

1. *обеспечение надлежащего баланса между зашитой информации о личности и требованиями свободного обмена информацией, свободы слова, свободы доступа к информации* – баланс между конфиденциальностью и прозрачностью. (Не следует забывать, что «баланс» - это неопределённое слово и все зависит от того, кто стремится установить баланс. С другой стороны, этот баланс имеет сложную структуру, поскольку должен основываться на учете законных и иногда конкурирующих интересов индивидов, организаций, собирающих и обрабатывающих персональные данные и общества в целом)[1];

2. *синхронизация новых технологий и организационных практик, их влияния на защиту персональных данных.* Такая политика должна быть не реактивной (непосредственная реакция на очевидные вызовы «сегодняшнего дня»), а проективной – технологически нейтральной и теоретически осмысленной;

3. *ценности информационной приватности:*

- *неприкосновенность цифровой сферы частной жизни индивида может рассматриваться либо как фундаментальная ценность, либо как инструментальная, обеспечение которой необходимо в целях защиты других прав индивидов или благосостояния общества;*
- *защита персональных данных может рассматриваться как единый комплекс (объект) регулирования или как совокупность проблем, каждая из которых регулируется в рамках различных законов, норм и правил (контекстуальная неприкосновенность)[2]. Отсюда, естественно, возникает вопрос, следует ли вообще вырабатывать какую-то единую политику по отношению к защите персональных данных;*

4. *меры обеспечения национальной* безопасности или доступа к информации - это угроза информационной сфере частной жизни; или наоборот: защита персональных данных – это препятствие реализации общественного интереса или обеспечению национальной безопасности;

5. *выбор позиции относительно международных инструментов регулирования* защиты персональных данных и методов:

- *защита персональных данных посредством технологической политики встроенной конфиденциальности;*
- *формирование «мирового порядка защиты персональных данных» на основе требований пересмотренной директивы Европейского союза;*
- *создание международного надзорного органа[3];*
- *выбор форм реализации международных норм на национальном уровне;*

6. *экономические аспекты и финансовые возможности* обеспечения защиты прав субъектов персональных данных;

1 Raab, Ch. (1999) Governing Privacy: Systems, Participants and Policy Instruments.
2 Schoeman, D. (1984) Philosophical Dimensions of Privacy: An Anthology. Доступно через: http://books.google.by/books/about/Philosophical_Dimensions_of_Privacy.html?id=q_FrmXyl3hUC&redir_esc=y.
3 Hert, P. (2013) Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency? Доступно через: http://moritzlaw.osu.edu/students/groups/is/files/2013/08/7-Hert-Papakonstantinou.pdf.

7. *технические возможности.*

Уровень политической поддержки или популярности позиций обуславливает ту или иную структуру «баланса» в различных социально-политических контекстах.

Та или иная политика в отношении защиты персональных данных может привести к одному из четырех сценариев:

- *общество тотального контроля и надзора, но не общество Большого брата, а общество децентрализованной сети, «узлы» которой как являются объектом контроля и надзора, так и сами контролируют других;*
- *фрагментированная мешанина норм, правил и законов защиты персональных данных в хаотических попытках ограничить все новые и новые практики контроля и надзора. Технологии, обеспечивающие приватность, будут широко использоваться для того, чтобы обеспечить анонимность. Давление потребителей будет вынуждать корпорации принимать все более строгие правила обращения с персональными данными и аудит в различных организациях. Но «победы приватности» будут кратковременными;*
- *общество имеющих приватность и лишенных ее. В некоторых странах будут существовать строгие законы защиты персональных данных. Проблема будет высоко политизирована. Органы, уполномоченные следить за защитой персональных данных, будут занимать ключевые позиции в управлении государством. Другие страны будут по-прежнему реагировать на проблемы приватности по мере их появления. Попытки введения глобальных норм и стандартов будут наталкиваться на сопротивление тех стран, которые буду получать дивиденды, становясь «раем для предоставления данных»;*
- *установление глобальных стандартов защиты данных для всех стран и компаний*[1].

Однако сама по себе задача установления баланса представляется проблематичной, поскольку:

- *конструирование баланса ценностей всегда осуществляется в интересах тех, кто принимает решения;*
- *нередко такой баланс основан на том, что защите персональных данных (и особенно контролю со стороны субъекта персональных данных) придается гораздо меньшее значение, чем другим, конфликтующим с ним, ценностям*[2]*;*
- *некоторые подходы к установлению баланса могут провоцировать дискриминацию: оказывать более серьезное негативное влияние на одних людей и создавать привилегии для других. Например, меры, предпринимаемые в целях обеспечения национальной безопасности, могут приводит к тому, что определённые «группы риска» будут иметь ограниченные гарантии защиты персональных данных.*

Известный специалист в сфере информационной приватности, профессор государственного управления и сравнительной политологии Эдинбургского университета Чарльз Рааб утверждает, что консенсус в отношении «баланса ценностей пока не достигнут даже на теоретическом уровне[3]. Поэтому аргументированное решение задачи защиты персональных данных – это всегда непростой процесс анализа последствий с учетом интересов различных сторон в конкретной ситуации. При этом

1 Там же.
2 Raab, C. (2014) Privacy as Security Value. Доступно через: http://bigdataandprivacy.org/wp-content/uploads/2014/08/Raab_PrivacySecurityValue.pdf.
3 Там же.

никакое решение не может быть окончательным. А широкое общественное обсуждение должно стать гарантией того, что новые вызовы и возможности ответов на них в достаточной степени учитываются при разработке стратегий.

Аргументированное решение задачи защиты персональных данных – это всегда непростой процесс анализа последствий с учетом интересов различных сторон в конкретной ситуации. При этом никакое решение не может быть окончательным. А широкое общественное обсуждение должно стать гарантией того, что новые вызовы и возможности ответов на них в достаточной степени учитываются при разработке стратегий

Как и любая другая публичная политика, политика в отношении защиты персональных данных определяется как «комплекс формальных и неформальных институтов, механизмов, отношений и процессов, существующих между и распространяющихся на государства, рынки, отдельных граждан и организации, как межправительственные, так и неправительственные, посредством которых на глобальном уровне определяются коллективные интересы, устанавливаются права и обязанности, разрешаются споры»[1], как коллективные усилия правительственных и неправительственных акторов с целью обнаружения, дальнейшего изучения или решения комплексных проблем, выходящих за рамки возможностей правительств (или других органов государственного управления)[2].

Обеспечение защиты персональных данных – это не обезличенный технический процесс выбора инструментов, а политический процесс, в котором принимают участие различные акторы с конфликтующими интересами, зачастую выходящими за рамки проблематики информационной приватности.

Политика в отношении персональных данных имеет многоуровневый и межсекторальный характер. В нее вовлечены наднациональные, национальные и субнациональные институты (государственные и неправительственные) и индивидуальные акторы.

Актор публичной политики – это «действующее лицо», которое принимает активное участие в процессе решения социально-значимых проблем и которое характеризуется, по крайней мере:

- *свободой маневра по отношению к принуждениям системы;*
- *способностью взаимодействия с другими;*
- *способность к активному поведению;*
- *наличием стратегии (цель и способы ее достижения);*
- *признанием со стороны других акторов*[3].

Политика в отношении персональных данных имеет многоуровневый и межсекторальный характер. В нее вовлечены наднациональные, национальные и субнаци-

1 Carlsson, I. et al. UN, Commission on Global Governance. (1995). Our Global Neighborhood. Доступно через: http://www.bibliotecapleyades.net/sociopolitica/sociopol_globalization05.htm.

2 Барабанов , О. (2009). Определение теоретических подходов. Проблемы глобального управления: выбор аналитической парадигмы. Вестник международных организаций: образование, наука, новая экономика. Доступно через: http://www.alleuropa.ru/index.php?option=com_content&task=view&id=1248.

3 В зависимости от того или иного подхода к политическому анализу, исследователи используют и по-разному определяют термины «агент действия», «субъект политики», «актор» и пр. Авторы данного пособия руководствуются определениями, обоснованными в книге Enserink, B., Hermans, L., Kwakkel, J., Thissen, W., Koppenjan, J. and Bots, P. (2010) Policy Analysis of Multi-Actor Systems. P. 79-108. Следует также отметить, что в рамках теории организаций чаще используется термин «стейкхолдер», который исторически предшествовал теоретическому оформлению понятия «актор политики».

ональные (государственные и неправительственные) акторы, как институциональные, так и индивидуальные.

Следует при этом отметить, что неправительственные акторы - это не только национальные неправительственные ассоциации и организации, но и трансграничные гражданские коалиции, «многосторонние платформы», частно-государственные партнерства, представители академического и технического сообществ[1], а также «конечные пользователи интернета», соблюдение прав которых является одним из основных принципов глобальной и европейской политики в области управления развитием и использованием сети интернет[2].

Существуют различные подходы к анализу сложной структуры акторов публичной политики[3]. Наиболее подходящим для первоначального введения в проблематику защиты персональных данных представляется структурирование на основании формальной/официальной позиции, предложенное Б.-Й. Коопсом и Ч. Раабом[4]. Исследователи, прежде всего, обращают внимание на то, что транснациональное «движение» персональных данных в глобальной сети обуславливает фундаментальное значение международных принципов и, следовательно, определяющую роль *глобальных и региональных межправительственных организаций* и объединений: ООН, ОЭСР, Совета Европы, Европейского союза, организации Азиатско-Тихоокеанского сотрудничества, Всемирного банка, Всемирной торговой организации, Международной торговой палаты и др.

Состав членов и цели каждой из вышеупомянутых международных организаций налагают свой отпечаток на содержание выдвигаемых ею инициатив в сфере защиты персональных данных. Тем не менее, в этих инициативах можно выделить ряд общих моментов, в совокупности составляющих общую стратегию экстерриториальной защиты персональных данных. Для того чтобы установить единообразный режим правового регулирования обработки и передачи персональных данных в рамках союза или сообщества стран, представляющая его международная организация, как правило, последовательно выполняет следующее:

- *добивается консенсуса стран-участниц данного сообщества относительно тех принципов защиты данных, которые должны применяться в рамках сообщества.*
- *легитимизирует эти принципы при помощи подписания странами-участницами соответствующего международного соглашения, предусматривающего обязанность стран-участниц гармонизировать свое национальное законодательство в соответствии с вышеуказанными принципами зашиты данных;*
- *устанавливает для стран-участниц, ратифицировавших вышеупомянутое международное соглашение и гармонизировавших национальное законодательство, режим наибольшего благоприятствования в сфере обмена персональными данными;*
- *запрещает (или, по крайней мере, строго ограничивает) обмен персональными данными со странами, не являющимися участницами данного международного соглашения о защите данных как напрямую, так и через третьи страны*[5].

1 Peters, A. (2009). Non-state actors as standard setters. Доступно через: https://ius.unibas.ch/uploads/publics/9591/20100219154311_4b7ea37fbba74.pdf.
2 Соколова, М.. (2011) Перспективы многостороннего диалога по вопросам управления развитием и использованием интернета в Республике Беларусь. Доступно через: http://ru.scribd.com/doc/86189304/sokolova
3 Подробно эти подходы описаны здесь Enserink, B., Hermans, L., Kwakkel, J., Thissen, W., Koppenjan, J. and Bots, P. (2010) Policy Analysis of Multi-Actor Systems.
4 Raab, C., Koops, B-J. (2009), Privacy Actors, Performances and the Future of Privacy Protection. Доступно через: http://www.research.ed.
5 Иванский, В.П. (1999) Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования. Доступно через: http://www.pravo.vuzlib.su/book_z137_page_1.html.

Международная торговая палата внимательно следит за инициативами международных организаций в области правового регулирования трансграничных потоков персональных данных и защиты приватности. Она уполномочена международными деловыми кругами на координацию лоббирования этих международных инициатив в нужном для бизнеса направлении. В 1981 г. Международная торговая палата учредила Комиссию по политике в области телекоммуникаций и информации, а также рабочую группу «Приватность и защита персональных данных» (Task Force on Privacy and Personal Data Protection), которая анализирует соответствующие проблемы и разрабатывает рекомендации для Международной торговой палаты по их решению этих[1]. Рабочая группа принимает активное участие в обсуждении реформы защиты персональных данных в Европейском союзе[2].

На национальном уровне важнейшую роль в разработке и реализации политики в отношении приватности, безусловно, играют *законодатели, суды и различные государственные органы.*

К числу ведущих институциональных акторов К. Беннет и Ч. Рааб относят также *уполномоченные органы по защите прав субъектов персональных данных и их международные объединения.*

Функции национального органа (или системы органов) по обеспечению качества персональных данных и защите прав субъектов данных (традиционно такие органы называют кратко: «органы защиты персональных данных»):

- *регистрационно-разрешительные,*
- *контрольно-надзорные,*
- *арбитражные,*
- *экспертные.*

Европейский инспектор по защите данных (Брюссель, edps.europa.eu)

Роль: защита персональных данных граждан, обрабатываемых в институтах и органах власти ЕС

В рамках своей работы институты ЕС могут хранить и обрабатывать персональные данные граждан и жителей ЕС, представленные в электронном и печатном виде, а также в видеоформате. В обязанности Европейского инспектора по защите данных входит защита персональных данных, частной жизни людей и пропаганда добросовестной работы в институтах и органах власти ЕС.

В чем заключается работа инспектора по защите данных в ЕС? Жесткий регламент ЕС служит руководством для институтов ЕС в отношении использования персональных данных жителей – например, имен, адресов, медицинских данных или трудового стажа. Защита данной информации является основополагающим

1 ICC Privacy Toolkit (2009). Доступно через: http://www.iccwbo.org/privacy_toolkit/.

2 ICC Response to the European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data. Доступно через: http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2009/ICC-Response-to-the-European-Commission-Consultation-on-the-Legal-Framework-for-the-Fundamental-Right-to-Protection-of-Personal-Data; Redline Version on New EU Standard Contractual Clauses for the Transfer of Personal Data on behalf of Hunton and Williams. Доступно через: http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2010/Redline-Version-on-New-EU-Standard-Contractual-Clauses-for-the-Transfer-of-Personal-Data-on-behalf-of-Hunton-and-Williams/; ICC Alternative Standard Contractual Clauses for the Transfer of Personal Data from the EU to Third Countries. Доступно через: http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2010/ICC-Alternative-Standard-Contractual-Clauses-for-the-Transfer-of-Personal-Data-from-the-EU-to-Third-Countries/, ICC discussion paper on data protection principle of accountability; ICC comments on EU General Data Protection Regulation Issues. Доступно через: http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2013/ICC-comments-EU-Gen-DP-Reg-Issues/; ICC discussion paper on data protection principle of accountability. Доступно через: http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2012/ICC-discussion-paper-on-data-protection-principle-of-accountability/.

правом. В штате каждого института ЕС имеется ответственный за защиту данных, который следит за исполнением соответствующих обязательств – например, данные могут быть обработаны только в силу особых причин и только на законных основаниях. Человек, данные о котором передаются на обработку, обладает законными правами, в частности, правом на внесение изменений в данные. Работа инспектора по защите данных заключается в контроле институтов ЕС и деятельности, направленной на защиту персональных данных и на обеспечение соответствия самым высоким стандартам в этой области. Инспектор по защите персональных данных также занимается рассмотрением и расследованием жалоб. Другие его обязанности включают:

- *мониторинг обработки данных в административных учреждениях ЕС;*
- *консультации по политике конфиденциальности и соответствующим законам;*
- *взаимодействие с аналогичными органами власти в странах-членах ЕС для обеспечения надёжной защиты данных.*

Как работает инспектор по защите персональных данных? Повседневная деятельность инспектора проходит в двух направлениях:

- *надзор и контроль за исполнением – оценка соблюдения стандартов по защите данных Европейскими институтами и организациями;*
- *консультационные и политические вопросы – консультации законодательных органов ЕС по проблемам защиты данных в рамках политической деятельности и новых законопроектов.*

Инспектор также осуществляет контроль над внедрением новых технологий, которые могут повлиять на защиту данных. Любой человек, посчитавший свои права ущемленными в ходе обработки личных данных в институтах или органах ЕС, может подать жалобу Инспектору по защите данных. Сделать это необходимо согласно форме подачи жалобы, размещенной на сайте инспектора по защите данных[1].

Основные требования, предъявляемые к национальному органу по защите данных международными соглашениями о гармонизации систем защиты данных:

- *компетентность. В виду быстрого усложнения информационно-коммуникационных технологий, с проблемой защиты персональных данных перестали справляться суды общего назначения («Пришло время, когда те, кто используют компьютеры для обработки персональной информации (независимо от того, насколько ответственными они являются), не могут больше оставлять на произвольное усмотрение одних лишь судей решение вопроса о том, адекватно ли защищают сферу частной жизнь их собственные компьютерные информационные системы»[2]);*
- *независимость. Государство с приходом компьютерных технологий оказалось одной из сторон, заинтересованных в обработке и использовании персональных данных, и, следовательно, ни один из государственных органов не в состоянии занимать позицию беспристрастного арбитра по отношению к коллизии прав субъекта данных и интересов владельцев/пользователей персональных данных. Независимость органа по защите данных в различных национальных правовых системах обеспечивается разнообразными средствами: статусом органа, его*

1 Европейская Комиссия. Генеральный директорат по коммуникациям (2013) Как работает Европейский Союз. Ваш гид по институтам ЕС. Доступно через: http://eeas.europa.eu/delegations/russia/documents/publications/how_eu_works_2013_ru.pdf.

2 Белая книга за 1975 г. с изложением позиции правительства Великобритании по проблеме защиты сферы частной жизни в связи с автоматизированной обработкой персональных данных. Цит. по: Wakes, R. Protection of Privacy.

местом в системе государственной власти, процедурой совместного назначения руководителя этого органа несколькими ветвями государственной власти, разделением административной подчиненности и подотчетности органа защиты данных между исполнительной и представительной ветвями власти, прямым указанием закона и многими другими методами.

В Австрии законом установлена двойная регулирующая структура, состоящая из Совета по защите данных и Комиссии по защите данных. В Финляндии в национальную систему органов по защите данных входят Омбудсмен по защите данных и Коллегия по защите данных. В Великобритании полномочия Регистратора по защите данных уравновешиваются полномочиями специализированного суда (трибунала) по защите данных, служащего апелляционной инстанцией, где можно опротестовать решения Регистратора. Несмотря на существование в ряде национально-правовых систем специализированных судов и трибуналов по защите данных, входящих в национальные системы органов по защите данных в качестве полноправных членов, суды общего назначения тоже сохраняют определенную роль в правовом регулировании обработки и использования персональных данных, входя практически во все национальные системы защиты данных в качестве «неявных» членов[1].

Национальные уполномоченные органы защиты прав субъектов персональных данных активно сотрудничают как на региональном, так и на международном уровнях.

- *Международная конференция членов комиссий по защите персональных данных (International Conference of Privacy and Data Protection Commissioners) (http://www.privacyconference2014.org/en/). Члены конференции принимают резолюции, а участие в конференциях открыто для всех желающих. Хотя из 85 стран, в которых есть соответствующие комиссии, только 59 аккредитованы на конференции, в ее работе участвуют 33 субнациональных комиссии из Австралии, Канады, Германии, Мексики, Испании и Швейцарии. Таким образом в составе конференции - 92 члена, а также Европейский инспектор по защите персональных данных (ЕС).*
- *Глобальная правоохранительная сеть по защите приватности (Global Privacy Enforcement Network) (https://www.privacyenforcement.net/) была создана в 2010 г. в соответствии с рекомендациями ОЭСР о трансграничном сотрудничестве в реализации законов, защищающих неприкосновенность частной жизни (2007 г.)[2]. Членами сети являются 26 стран.*
- *Региональная организация «Рабочая группа «Статья 29»» (Article 29 Working Party) (http://ec.europa.eu/justice/data-protection/article-29/index_en.htm) – одна из наиболее влиятельных организаций, поскольку она:*
    - формально институционализирована в рамках Директивы ЕС о защите персональных данных (1995);
    - рассматривает чрезвычайно широкий круг проблем;
    - играет важную роль в процессе модернизации Конвенции Совета Европы о защите персональных данных.

Несмотря на то что рабочая группа имеет статус рекомендательного органа, национальные органы защиты персональных данных внимательно изучают разработанные ее экспертами документы.

1 Иванский, В. (1999) Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования. Доступно через: http://www.pravo.vuzlib.su/book_z137_page_1.html.

2 OECD (2007) Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy. Доступно через: http://www.oecd.org/internet/ieconomy/oecdrecommendationoncross-borderco-operationintheenforcementoflawsprotectingprivacy.htm.

- *Европейский инспектор по защите прав субъектов персональных данных (European Data Protection Supervisor) контролирует соблюдение прав граждан в процессе сбора, обработки, хранения и передачи персональных данных.*
- *Конференция европейских органов по защите личных данных (European Data Protection Authorities) (http://www.coe.int/t/dghl/standardsetting/dataprotection/european-conference/). Принимаемые на конференции резолюции имеют существенное значение для разработки политики защиты персональных данных. Членом конференции могут быть органы только тех стран, которые подписали Конвенцию Совета Европы о защите персональных данных или ратифицировали Директиву Европейского союза 1995 г.*
- *Сеть организаций защиты персональных данных Центральной и Восточной Европы (Central and Eastern Europe Data Protection Authorities (CEEDPA)) (http://www.ceecprivacy.org/main.php) CEEDPA была создана в 2001 году. В соответствии с Варшавской декларацией, подписанной 17 декабря 2001 г., цель организации заключается в обмене информацией и положительным практическим опытом в области защиты персональных данных, гармонизации национальных законодательств, регулирующих вопросы защиты прав субъектов персональных данных, с законодательством ЕС. В состав CEEDPA входят: Албания, Болгария, Босния и Герцеговина, Венгрия, Латвия, Литва, Македония, Молдова, Польша, Российская Федерация, Румыния, Сербия, Словакия, Украина, Хорватия, Черногория, Чехия, Эстония.*
- *Консорциум «ФЕДРА» (PHAEDRA, Improving Practical and Helpful Co-operation between Data Protection Authorities). Цель консорциума – содействовать сотрудничеству и координации деятельности органов защиты персональных данных в различных странах Членами «ФЕДРА» являются Брюссельский свободный университет, Лондонская Трехсторонняя исследовательская и консультационная компания (Trilateral Research & Consulting), Главный инспектор по защите персональных данных Польши и Первый Каталонский университет Святого Жауме. В качестве главного механизма сотрудничества «ФЕДРА» провозглашает принцип децентрализации и координации. Реализация этого принципа означает создание особого юридического пространства широких и многократно пересекающихся юрисдикций («large and cross multiple jurisdictions»)*[1].
- *Ассоциация уполномоченных органов по защите прав субъектов персональных данных северных стран (Nordic Data Protection Authorities) (NDPA), в которую входят Дания, Норвегия, Швеция, Финляндия.*
- *Ассоциация франкофонных уполномоченных органов по защите прав субъектов персональных данных (Association of Francophone Data Protection Authorities (AFAPDP)) (http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2416#, http://www.privacycommission.be/en/afapdp-conference).*
- *Ассоциация британских, ирландских уполномоченных и уполномоченных островов (British, Irish and Islands Data Protection Authorities (BIIDPA)).*
- *Ассоциация уполномоченных азиатско-тихоокеанского региона (Asia Pasific Privacy Authorities (APPA) (http://www.appaforum.org/).*
- *Азиатско-тихоокеанское объединение трансграничной правой защиты персональных данных (APEC Cross-Border Privacy Enforcement Arrangement (CPEA))*

1 Егошина, Г. (2014) Модернизация конституционно-правового регулирования защиты персональных данных в Европе: усиление региональной интеграции. Доступно через: http://teoria-practica.ru/rus/files/arhiv_zhurnala/2014/3/yurisprudentsiya/egoshina.pdf.

(http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx).

- *Латино-американская сеть уполномоченных (Latin American Network (RIPD ReDIPD)) (http://itlaw.wikia.com/wiki/Ibero-American_Data_Protection_Network).*

Очевидно, что и *различные государственные учреждения*, обеспечивающие процессы сбора, хранения и обработки данных также существенно влияют на политику в отношении защиты персональных данных. Их роль и влияние определяются функциями в различных контекстах (см., таблицу «Пример: функции и контексты акторов политики в отношении защиты персональных данных»).

Таблица. Пример: функции и контексты акторов политики в отношении защиты персональных данных

Функции	**Контексты**
Сбор данных	Бизнес, торговля
Хранение данных	Полиция
Обмен данными	Слежение
Извлечение данных	Транспорт
	Здравоохранение
	Социальное обеспечение
	Финансы

Неправительственные институциональные акторы – крупные интернет-компании (в лице ответственных или департаментов по защите прав субъектов персональных данных) составляют еще одну влиятельную группу акторов. Так, в 1983 г. была создана Международная рабочая группа по защите персональных данных в сфере телекоммуникаций (Берлинская группа), которая опубликовала ряд влиятельных в рамках европейской политики документов[1]. Альянс онлайн-приватности (Online Privacy Alliance: http://www.privacyalliance.org/) – бизнес-ассоциация, содействующая разработке правил и принципов саморегулирования в целях обеспечения защиты персональных данных потребителей. В 2008 г. была создана ассоциация «Глобальная сетевая инициатива» (Global network initiative: https://www.globalnetworkinitiative.org/), члены которой в рамках стратегий социальной корпоративной ответственности разрабатывают критерии и меры обеспечения защиты персональных данных в сфере ИКТ-индустрии. Рабочая группа по приватности и защите персональных данных Международной торговой палаты – единственная бизнес-ассоциация, имеющая статус наблюдателя в комитете по защите персональных данных Совета Европы[2].

Группы активистов защиты прав субъектов персональных данных формируются и функционируют на национальном и наднациональном уровнях. Такие организации, как «Electronic Privacy Information Center», «Privacy International» оказывают существенное влияние на формирования принципов и механизмов регулирования. Особый интерес, с точки зрения экспертов, представляет организация «Европейские

1 International Working Group on Data Protection in Telecommunications. Доступно через: http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt.

2 International chamber of commerce (2008) Privacy and Personal Data. Доступно через: http://www.iccwbo.org/advocacy-codes-and-rules/areas-of-work/digitaleconomy/privacy-and-personal-data-protection.

цифровые права» (European Digital Rights/EDRI), созданная в 2002 г. и объединяющая 29 групп из 18 европейских стран[1]. В частности, EDRI подготовила популярную брошюру «Защита персональных данных. Введение»[2].

Серьезным вкладом в обеспечение прав субъектов персональных данных стали Международные принципы применения прав человека в отношении мониторинга средств связи, которые были разработаны общественными организациями («Access», «Article 19», «Association for Progressive Communications», «Bits of Freedom», «Electronic Frontier Foundation», «European Digital Rights», «Privacy International» и др.)[3]

Среди влиятельных акторов – *организации, устанавливающие технические стандарты:*

- *Международная организация стандартизации,*
- *Форум информационной безопасности (https://www.securityforum.org/)[4],*
- *Европейский комитет стандартизации (http://www.cenelec.eu/),*
- *Британский институт стандартов http://www.bsigroup.com/en-GB/[5].*

Хотя в процессе обсуждения и принятия решений относительно политики защиты прав субъектов персональных данных участвуют разнообразные акторы (см. таблицу «Основные акторы политики в отношении персональных данных»), главную роль все же играют регулирующие органы, разработчики и поставщики технологий, контролеры и субъекты данных, политики и гражданские объединения.

Таблица. Основные акторы политики в отношении персональных данных[6]

Актор	Функция
Разработчик конституции	Обеспечивает право на приватность (и защиту персональных данных)
Законодатель	Разрабатывает закон о защите персональных данных, а также другие законодательные акты с учетом права субъекта данных на защиту персональных данных

1 Raab, C, Koops, B-J (2009), Privacy Actors, Performances and the Future of Privacy Protection. Доступно через: http://www.research.ed.ac.uk/portal/files/12592176/Privacy_Actors_Performances_and_the_Future_of_Privacy_Protection.pdf.
2 EDRI (2012) Защита персональных данных. Введение. Доступно через: http://www.lawtrend.org/information-access/zashhita-dannyh.
3 International Principles on the Application of Human Rights to Communications Surveillance. Доступно через: https://en.necessaryandproportionate.org/.
4 The Standard of Good Practice for Information Security, Information Security Forum (2003). Доступно через: http://www.netbotz.com/library/Info_Security_Forum_Standard_Good_Practices.pdf.
5 BS 7799-3:2006.Standard on Information Security Management Systems-Guidelines for Information Security Risk Management. Доступно через: http://www.iso.staratel.com/ISO17799/Doc/BS7799.3.1999/BS%207799-3-2006.pdf.
6 Raab, C., Koops, B-J (2009) ‘Privacy Actors, Performances and the Future of Privacy Protection. Доступно через: http://www.research.ed.ac.uk/portal/files/12592176/Privacy_Actors_Performances_and_the_Future_of_Privacy_Protection.pdf.

Актор	Функция
Уполномоченный орган по защите прав субъектов персональных данных	Контролирует исполнение законов, способствует распространению лучших практик, инициирует привлечение внимания общественности к вопросам защиты персональных данных
Контролеры данных	Принимают решения относительно целей обработки и типа данных, которые должны быть обработаны
Сотрудники государственных органов	Исполнение законов, обучение персонала правилам и принципом защиты прав субъектов персональных данных
Частные компании	Исполнение законов, обучение персонала правилам и принципом защиты прав субъектов персональных данных, разработка и исполнение корпоративных кодексов, лоббирование тех или иных решений
Гражданские ассоциации, группы активистов	Борются за защиту прав субъектов персональных данных, предлагают решения, рекомендуют, привлекают внимание общественности
Академическое сообщество (правоведы, социологи, философы)	Исследование и проблем защиты прав субъектов персональных данных, выявление долговременных тенденций, прогнозы, рекомендации
Журналисты	Освещают события и проблемы, объясняют политику и тенденции развития, обнародуют факты нарушения прав субъектов данных
Субъекты данных (граждане, потребители)	Защищают свое право на приватность информационной сферы, жалуются
Разработчики технических стандартов и технологий	Разрабатывают стандарты и решения, обеспечивающие защиту персональных данных, обучают специалистов в сфере ИТ

В процессе принятия решений, разработки и реализации политики складываются и разные конфигурации интересов акторов. Эксперты утверждают, что только серьезный анализ таких кластеров интересов позволяет эффективно решать проблемы защиты прав субъектов данных в конкретных ситуациях. Без учета этого положение будет нестабильным, мозаика несовместимых интересов и ресурсов будет порождать нереализуемые стратегии, каждый инструмент будет использоваться изолированно. Итог – отсутствие единой цели и, следовательно, эффективной политики, основанной на синергии регуляторных воздействий.

ИНСТРУМЕНТЫ ПОЛИТИКИ В ОТНОШЕНИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Набор инструментов политики в отношении защиты персональных данных включает не только меры законодательного регулирования, но и транснациональные принципы, руководства и соглашения, практики саморегулирования, стандартизации, технологические решения и просветительские мероприятия. Закон должен дополняться кодексами поведения и технологическими мерами, опираться на соответствующую организационную культуру и поддержку общественности

Формальный нормативный базис законодательства о защите персональных данных составляют фундаментальные права человека, зафиксированные в международных и региональных документах:

- *Всеобщей декларации прав человека (ООН, 1948) ст. 19, 29;*
- *Международном пакте о гражданских и политических правах (ст. 15) (ООН, 1966);*
- *Международном пакте об экономических, социальных и культурных правах (ООН, 1976);*
- *Международной конвенции о ликвидации всех форм расовой дискриминации (ст.5);*
- *Международной конвенции о ликвидации всех форм дискриминации женщин (1965 г.);*
- *Конвенции о защите прав человека и основных свобод (Совет Европы, 1950, ст. 10, 15, 16, 17);*
- *Американской декларация прав и свобод человека (1948 (ст. 6);*
- *Американской конвенция о правах человека (Пакт Сан-Хосе, 1969 г.,) (ст. 13);*
- *Африканской Хартия прав человека и народов (Организация африканского единства, 1981, ст. 9, 27, 29);*
- *Хартии социальных прав и гарантий граждан независимых государств (СНГ, 1994);*
- *Хартии Европейского союза об основных правах человека (ЕС, 2000);*
- *Арабской хартии прав человека (Лига арабских государств, 2004);*
- *Конвенции Содружества Независимых Государств о правах и основных свободах человека (СНГ, 2011);*
- *Азиатской хартии по правам человека (АСЕАН, 2012);*
- *Бишкекской декларация ОБСЕ.*

Международное соглашение на глобальном уровне о принципах защиты персональных данных до сих пор отсутствует, хотя эксперты все более настойчиво говорят о необходимости разработки такого документа.

В настоящее время эту лакуну заполняют:

- *Резолюция Генеральной Ассамблеи ООН «Право на приватность в цифровую эпоху» (2014);*

- *Резолюция Генеральной Ассамблеи ООН «Руководящие принципы, касающиеся компьютеризированных картотек, содержащих данные личного характера» (1990);*
- *Конвенция № 108 Совета Европы о защите индивидуумов (частных лиц) по отношению к автоматизированной обработке персональных данных (1981) и Дополнительный протокол, которые вышла за рамки регионального документа и открыта для подписания неевропейскими странами;*
- *Рекомендации в отношении Руководящих принципов по защите неприкосновенности частной жизни и трансграничных потоков персональных данных Организации экономического сотрудничества и развития.*

Особое место в этом контексте занимает Директива № 95/46/ЕС Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных»[1], которая, по мнению экспертов, определяет основные тенденции законодательного регулирования защиты персональных данных, поскольку:

- *принцип адекватности национальных законов требованиям Директивы определяет возможности обмена данными со странами Европейского союза,*
- *требования Директивы № 95/46/ЕС дублируются в Дополнительном протоколе Конвенция № 108 Совета Европы[2].*

Таблица. *Принципы защиты данных в международных документах[3].*

Принципы защиты данных	Конвенция Совета Европы	Руководящие принципы ОЭСР	Директива ЕС о защите данных
Честные и законные средства сбора данных	+	+	+
Указанные и законные цели сбора данных	+	+	+
Соответствие данных цели их сбора	+	+	+
Точность данных	+	+	+
Хранение данных только до момента достижения цели их сбора	+	-	+
Особый режим обращения с «уязвимыми данными»	+	-	+

1 Директива Европейского парламента и Совета Европейского союза 95/46/ЕС от 24 октября 1995 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных (в редакции Регламента Европейского парламента и Совета ЕС 1882/2003 от 29 сентября 2003 года) http://pd.rkn.gov.ru/docs/Direktiva_Evropejskogo_Parlamenta_i_Soveta_Evropejskogo_Sojuz_95_46_ES.rtf.

2 Подробно содержание документов будет рассмотрено в разделах, посвященных правовым аспектам защиты персональных данных.

3 Tan J (2008) A comparative study of the APEC privacy framework: A new voice in the data protection dialogue?. In Asian Journal of Comparative Law, 3(1). http://www.degruyter.com/dg/viewarticle/j$002fasjcl.2008.3.1$002fasjcl.2008.3.1.1071$002fasjcl.2008.3.1.1071.xml;jsessionid=F36717919BBF04391AC61CF44A516545.

Принципы защиты данных	Конвенция Совета Европы	Руководящие принципы ОЭСР	Директива ЕС о защите данных
Безопасность обработки и хранения данных	+	+	+
Информирование субъекта данных об осуществлении обработки его данных	+	+	+
Доступ субъекта данных к своим личным данным и возможность их изменения	+	+	+
Подотчетность при обработке данных	+	+	+

Международные принципы защиты персональных данных – не статичный инструмент. С появлением новых технологий, осознанием новых вызовов производится их периодический пересмотр.

В 2013 г. была опубликована новая редакция Руководящих принципов ОЭСР.

В новой редакции сохранены все основные принципы:

- *законный и ограниченный сбор персональных данных, получаемых с ведома и согласия физического лица,*
- *данные собираются в соответствии с целями обработки, обеспечивается их полнота и актуализация,*
- *использование данных для новых целей должно быть либо совместимо с первоначальной целью обработки, либо на новые виды использования или раскрытия информации требуется согласие,*
- *разумные меры безопасности для защиты данных и обеспечивается подотчетность всех операторов данных,*
- *у субъекта персональных данных есть право на доступ к хранящимся о нем данным, а также право на их уничтожение или исправление.*

Вместе с тем в новой редакции усиливаются требования к подотчетности оператора данных независимо от местонахождения данных, а также независимо от того, обрабатываются ли данные самим оператором, его представителями или передаются другому оператору.

Рекомендации ОЭСР (2013)

Акцент на требованиях подотчетности оператора данных независимо от местонахождения данных, а также независимо от того, обрабатываются ли данные самим оператором, его представителями или передаются другому оператору.

Управление глобальными рисками информационной приватности требует разработки национальных стратегий стран с целью координирования усилий всех акторов на государственном уровне и активизации сотрудничества между уполномоченными органами по защите персональных данных

ОЭСР рекомендует:

- *использовать адаптированные под особенности организации программы управления защитой персональных данных и оценки последствий утечек для управления связанными с утечками рисками;*
- *включать в контракты положения, требующие соблюдения политики оператора данных по вопросам защиты персональных данных;*
- *устанавливать протоколы оповещения в случае инцидентов безопасности;*
- *разрабатывать план реагирования на инциденты безопасности и запросы со стороны субъекта персональных данных.*
- *Руководство ОЭСР исходит из того, что управление глобальными рисками требует разработки национальных стратегий стран с целью координирования усилий всех акторов на государственном уровне и активизации сотрудничества между уполномоченными органами по защите персональных данных.*

В настоящее время ведется работа по модернизации регулирования защиты персональных данных в Европейском союзе[1].

В отличие от многих других сфер управления специфика возникновения и развития интернета как распределенной, «саморегулирующейся» и «саморазвивающейся» сети не позволяет сводить вопросы упорядочивания соответствующих общественных отношений к формулированию «желательных» управляющих воздействий и их фиксации в виде норм права. Иначе говоря, управление путем принятия неких норм национального законодательства или международных соглашений абсолютно бесперспективно[2].

Поэтому саморегулирование в рамках интернет-бизнеса и различных организаций (в том числе и государственных) является одним из важнейших инструментов в политики защиты персональных данных. Связано это прежде всего с тем, что в ситуации быстрых технологических изменений, неопределённости отношений юрисдикций при трансграничной передаче персональных данных посредством глобальных телекоммуникационных сетей, национальное законодательство в принципе не в состоянии обеспечить надлежащий уровень информационной приватности человека.

> *Саморегулирование в рамках интернет-бизнеса и различных организаций (в том числе и государственных) является одним из важнейших инструментов в политики защиты персональных данных*

Основные формы саморегулирования – это обязательства, кодексы, стандарты, корпоративные правила.

Мотивацию саморегулирования в сфере защиты персональных данных можно суммировать следующим образом. Различные учреждения и институты посредством саморегулирования стремятся:

- *избежать законодательных мер;*
- *предупредить разработку законодательных мер;*
- *заполнить пробелы в законодательстве;*
- *более эффективно реализовать нормы законодательства.*

Инструменты саморегулирования могут разрабатываться на уровне:

- *организации (государственной, частной, общественной, международной, национальной);*

1 Подробно об это см. в разделе «Международные принципы и стандарты».
2 Курбалийя, Й. (2010) Управление Интернетом. Доступно через: http://cctld.ru/files/IG-2010.pdf.

- *сектора экономики;*
- *профессионального сообщества (например, для технических специалистов, которые занимаются обработкой информации, технологические кодексы предписывают определенные нормы для разного рода приложений).*

Существуют различные пути принятия компаниями, организациями или отраслями мер саморегулирования в области защиты персональных данных:

- *информирование об обязательствах;*
- *введение внутренних руководящих указаний или принципов;*
- *принятие Кодексов практики или поведения;*
- *учреждение должности специального ответственного.*

Обязательства – это краткие констатации минимальных мер по защите персональных данных, обеспечение которых гарантирует та или иная организация (государственная, частная, общественная).

Кодексы поведения – важнейший инструмент политики даже в тех странах, где существует достаточно эффективное законодательство, поскольку:

- *они позволяют организациям публично представить свою политику и обеспечить необходимую прозрачность с персональными данными;*
- *они содействуют правильному применению мер, определенных законодательством;*
- *процедура обсуждения кодексов содействует более глубокому пониманию проблем защиты персональных данных в различных сферах;*
- *кодексы – достаточно гибкие инструменты и легко могут изменяться с изменением технологических или экономических условий.*

> *Кодексы поведения – важнейший инструмент политики даже при наличии эффективного законодательства, поскольку позволяют организациям публично представить свою политику и обеспечить необходимую прозрачность с персональными данными; содействуют правильному применению мер, определенных законодательством; процедура обсуждения кодексов содействует более глубокому пониманию проблем защиты персональных данных в различных сферах; достаточно гибкие инструменты и легко могут изменяться с изменением технологических или экономических условий*

Директива ЕС от 24 октября 1995 о защите персональных данных выводит кодексы практики/поведения на международный уровень. В ст. 20 говорится:

> *«...страны-участницы должны поощрять заинтересованные деловые круги к участию в разработке европейских Кодексов поведения или профессиональной этики в отношении определенных отраслей деятельности на основе принципов, установленных в настоящей Директиве»*[1].

В области защиты персональных данных форма, содержание и основная направленность кодексов практики/поведения не являются единообразными.

Анализ, проведенный ОЭСР, показывает, что в основе большинства кодексов лежит принцип «соблюдай или объясни»: хотя они и содержат некоторые обязательные принципы, большинство рекомендаций по своей сути не носит обязательного ха-

1 European Union. Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Brussels: European Commission, OJ No. L281.24, October 1995.

рактера и позволяют выбрать иной подход; в этом случае компании должны дать надлежащие объяснения[1].

Одним из ключевых элементов любого кодекса практики/поведения должен быть его добровольный характер. Соответственно, любой кодекс не предоставляет никаких законных прав другим сторонам, вовлеченным в процесс обработки, передачи и использования персональных данных. Например, субъекты данных или лицо, передающее данные, не обретают никаких прав против владельца данных, который создал конкретный кодекс. Однако это не препятствует кодексу быть обязательным для исполнения внутри данной отрасли или корпорации. Например, нарушение отраслевых стандартов, содержащихся в кодексах, может привести к прекращению членства их нарушителя в соответствующей отраслевой или профессиональной ассоциации.

Если кодекс просто провозглашает широкие принципы защиты данных, но затем не предлагает мер для соблюдения этих принципов, то такой кодекс не является средством защиты данных.

Следует отметить, что кодексы поведения/практики являются обычно инструментами частного сектора. Этому способствуют несколько причин:

- *регулирование защиты данных государственного сектора обычно осуществляется на основании правил, установленных внутренними инструкциями;*
- *в большинстве стран защита данных частного сектора остается сравнительно нерегулируемой, что предоставляет отраслям и корпорациям возможности для саморегулирования*.

Исторически сложилось так, что многие кодексы ограничиваются рамками отдельных секторов бизнеса. Прежде всего, в банковской и страховой отраслях, поскольку именно здесь собирают громадные количества персональных данных и располагают технологическими возможностями для их обработки. Кроме того, эти отрасли могут быть внутренне взаимосвязаны через корпоративное право собственности и могут иметь интересы в смежных областях бизнеса (например, службы безопасности торговли), тем самым потенциально способствовать еще большей концентрации данных. В рамках индустрия прямого маркетинга, строящегося на использовании информации о потребителях, создание кодексов практики/поведения также стало общепринятой практикой.

Существуют и межотраслевые кодексы. Национальный компьютерный центр Великобритании разработал ряд кодексов, относящихся к: (1) службам безопасности; (2) компьютерным бюро; (3) данным о наемных служащих; (4) управлению собственностью; (5) информации о потребителях и поставщиках.

Кодексы поведения в отношении защиты персональных данных имеют и международные организации. Свод практических правил Международной Организации Труда (International Labour Organization – ILO) по защите персональных данных работника был принят на совещании экспертов в 1996 г. Кодекс не имеет обязательной силы, но может быть использован при разработке национального законодательства. В нем изложены основные принципы сбора, обработки, использования и хранения личной информации о работниках, а также о лицах, обращающихся к работодателю в целях трудоустройства. Специальные разделы Свода посвящены личным правам работника, возникающим в связи со сбором персональных данных, в частности, праву на уведомление о сборе персональных данных, на ознакомление в рабочее время со сведениями о себе, которые имеются у работодателя, на получение копий документов, право на доступ к медицинским документам через своего

1 Ваимерш, Э. (2013) Европейские кодексы корпоративного управления и их эффективность http://www.oecd.org/daf/ca/2013OECDRussiaCorporateGovernanceRoundtableEuropeanCodesRus.pdf.

врача-представителя и др. Эти требования могут служить надежным ориентиром при принятии конкретных решений в отношении защиты личных данных работников и содействовать разработке соответствующего национального законодательства.

Как и законодательное регулирование, кодексы поведения имеют свои ограничения. Анализ достоинств и недостатков этой формы саморегулирования, проведенный ОЭСР, остается актуальным и сейчас.

Достоинства саморегулирования:

- *кодексы поведения доказали, что они могут быть весьма гибкими инструментами для внедрения закона в конкретные отрасли и сектора экономики;*
- *релевантные процедуры обладают весьма позитивным воздействием на взаимосвязь палаты с различными отраслями и секторами экономики;*
- *и те, и другие ведут к улучшенному осознанию и пониманию проблем и вопросов защиты персональных данных, которые являются специфическими для каждой отрасли или сектора экономики;*
- *Кодексы поведения предоставляют определенным отраслям удобную возможность продемонстрировать реальную заботу о вопросах защиты права на невмешательство в частную жизнь;*
- *отрасли и сектора, подлежащие регулированию кодексом, наделенным правовой санкцией, могут служить примером и посредником для других.*

Недостатки саморегулирования

- *регулирование при помощи кодексов может быть ограничено условиями конкуренции и другими аспектами некоего конкретного сектора или отрасли;*
- *Кодексы поведения могут усложнить или запутать правовые рамки, которые применяются в конкретном секторе или отрасли;*
- *субъекты данных не всегда осведомлены о статусе конкретного Кодекса поведения: наделен он правовой санкцией или нет;*
- *требование адекватных консультаций может создать проблемы с поиском достаточно компетентного партнера;*
- *практический эффект любого кодекса может зависеть соответственно от сферы его компетенции и статуса, а также иных специфических условий*[1].

Стандарты – это не только технические критерии надежности степени защиты персональных данных, но и инструменты реализации политики в этой сфере

Стандарты – это не только технические критерии надежности степени защиты персональных данных, но и инструменты реализации политики в этой сфере. Ведь стандартизация, по сути, представляет собой общепринятую процедуру оценки, которая позволяет определить, действительно ли организация делает то, что провозглашает в качестве правил, и включает три компонента:

- *установление технических стандартов;*
- *установление стандартов процедур обработки (менеджмента);*

1 OECD documents. Privacy and data rotection: Issues and Challenges",Information Computer Communication Policy. Organisation for Economic Cooperation and Development, Paris, 1966, p. 46 -47.

- *процедуры оценки влияние тех или иных технологий на защиту персональных данных*[1].

Разработкой стандартов в этой сфере наряду с Международной организацией стандартизации (ISO) занимается Европейский комитет по стандартизации (The Centre Européanne de Normalisations (CEN). Вместе с рабочей группой «Article 29» они контролируют выполнение Директивы ЕС 1995 г., устанавливая и контролируя стандарты в трех сферах:

- *общий стандарт защиты персональных данных (практические меры, которые организации должны реализовать для выполнения требований директивы);*
- *секторальные стандарты (информация в сфере здравоохранения и пр.);*
- *стандарты для специфических задач (главным образом, в онлайн-среде).*

Сертификация (получение сертификатов соответствия стандартам) конкретизирует требования и делает более продуктивной процедуру аудита и проверки на соответствие требованиям[2].

Оценка влияния на защиту персональных данных – это, по сути, оценка возможных рисков.

Ясные критерии оценки риска для защиты данных при введении тех или иных процедур частными и государственными учреждениями позволяют предупредить возможные нарушения законодательства и позволяют общественности предусмотреть возможные угрозы информационной приватности.

Такая оценка должна осуществляться в соответствии с определенными правилами и учитывать:

- *тип персональных данных, которые подвергаются риску,*
- *источник, из которого будет получаться информация,*
- *обстоятельства сбора информации,*
- *процесс обработки персональных данных,*
- *предполагаемое использование имеющихся или производимых персональных данных,*
- *предполагаемых реципиентов и способы использования ими информации,*
- *обстоятельства, при которых производится информация,*
- *при каких условиях возможны использование и раскрытие информации,*
- *меры по недопущению неавторизованного доступа, раскрытии, модификации или уничтожения*[3].

К инструментам политики защиты персональных данных аналитики относят и технологии, обеспечивающие приватность на основе принципа «проектируемой конфиденциальности».

1 ISO 22307:2008 on Financial Services: Privacy Impact Assessment (ISO 22307:2008 Финансовые услуги. Оценка влияния конфиденциальности); ISO 9564-1:2002, Banking–PIN Management and Security–Part 1: Basic Principles and Requirements for Online PIN Handling in ATM and POS Systems; ISO 18043:2006, Information Technology–Security Techniques–Selection,Deployment and Operations of Intrusion Detection Systems ИСО/МЭК 18043:2006 'Информационные технологии - Методы гарантии безопасности http://vsegost.com/Catalog/57/5736.shtml.

2 Winn, J. (2008) Technical Standards as Data Protection Regulation. Доступно через: http://dx.doi.org/10.2139/ssrn.1118542

3 Bennett, C. (2001) What government should know about privacy: a foundation paper. Доступно через: http://www.colinbennett.ca/wp-content/uploads/2012/06/What-Government-Should-Know-about-Privacy.pdf

Заложенная при проектировании защита персональных данных (privacy by design) - это концепция, которая исходит из того, что. защита личной информации, не может быть обеспечена исключительно соблюдением нормативно-правовых актов.

Заложенная при проектировании защита персональных данных (privacy by design) – это концепция, которая исходит из того, что защита личной информации не может быть обеспечена исключительно соблюдением нормативно-правовых актов.

Такая защита должна стать «правилом по умолчанию» в работе любой организации, что означает:

встраивание конфиденциальности в конструкцию системы должно быть активным, а не ограничиваться лишь мерами по устранению последствий. Личная информация должна быть защищена до того, как система запущена в работу, а не после выявления нарушений конфиденциальности;

конфиденциальность как стандартная установка. Параметры по умолчанию часто являются определяющими (многие пользователи вообще их никогда не меняют). Поэтому необходимо обеспечить максимальный «автоматизм» в той или иной информационной системе или деловых отношениях: не требуется никаких действий со стороны индивидуума для защиты личной информации, – система уже изначально содержит в себе необходимые установки;

конфиденциальность как часть структуры. Защита личной информации должна стать неотъемлемой частью архитектуры любой информационной системы или деловых отношений;

полная функциональность с суммарным положительным результатом – *учет всех законных интересов и целей «беспроигрышным» способом, без ненужных компромиссов* (например, укрепление безопасности системы в противовес защите личной информации), демонстрируя, что можно обеспечить и то, и другое;

защита личной информации на протяжении всего цикла ее сбора, хранения, обработки и уничтожения;

доступность и открытость – гарантии того, что система действительно работает в соответствии с заявленными принципами и целями (это должно быть подтверждено независимой проверкой). Все компоненты и операции остаются открытыми и доступными, как для пользователей, так и для тех, кто обеспечивает сервис;

соблюдение конфиденциальности пользователей. Система должна быть ориентирована, в первую очередь, на пользователя: защита личной информации по умолчанию, своевременное уведомление о сборе личной информации, предоставление пользователю свободы выбора в удобной и понятной форме[1].

Наиболее распространенные технологические инструменты, обеспечивающие защиту персональных данных – это шифрование, технологии анонимизации и «псевдонимизации», фильтры.

Технологии, как и другие инструменты политики защиты персональных данных, имеют недостатки. Прежде всего, пользователю иногда бывает сложно узнать или понять, правильно ли работает технология. Можно заметить сигналы нарушения приватности: сомнительные электронные сообщения, появление персональной информации в интернете и пр. Но вряд ли возможно с абсолютной уверенностью утверждать, что с технической точки зрения приватность обеспечена. Более того,

1 Кавукиан, Э. (2011) Privacy by Design 7 основополагающих принципов. Доступно через: http://privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-russian.pdf.

даже если, ошибки и сбои обнаруживаются и исправляются специалистами, обычно сложно узнать, внесены ли изменения технически корректным способом.

> *Информирование и образование граждан – важный инструмент в работе регулирующих органов, неправительственных организаций, политических партий*

Законы, кодексы, технологический дизайн не в состоянии обеспечить защиту персональных данных, если индивиды не умеют предотвратить вмешательство в цифровую сферу частной жизни. Информирование и образование граждан – важный инструмент в работе регулирующих органов, неправительственных организаций, политических партий. Однако просвещение в сфере защиты персональных данных – это не только обучение технологиям, но и пропаганда социальных норм, ответственного поведения в отношении как своих данных, так и информации о других.

Политика в отношении персональных данных имеет многоуровневый и межсекторальный характер. В нее вовлечены наднациональные, национальные и субнациональные (государственные и неправительственные) акторы, как институциональные, так и индивидуальные.

В процессе принятия решений, разработки и реализации политики складываются и разные конфигурации интересов акторов. Только серьезный анализ таких кластеров интересов позволяет эффективно решать проблемы защиты прав субъектов данных в конкретных ситуациях. Без учета этого положение будет нестабильным, мозаика несовместимых интересов и ресурсов будет порождать нереализуемые стратегии, каждый инструмент будет использоваться изолированно. Итог – отсутствие единой цели и, следовательно, эффективной политики, основанной на синергии регуляторных воздействий.

Набор инструментов политики в отношении защиты персональных данных включает не только меры законодательного регулирования, но и транснациональные принципы, руководства и соглашения, практики саморегулирования, стандартизации, технологические решения и просветительские мероприятия. Закон должен дополняться кодексами поведения и технологическими мерами, опираться на соответствующую организационную культуру и поддержку общественности.

Управление глобальными рисками информационной приватности требует:

- *соблюдения принципов законности, конкретизации целей, минимизации сбора и использования персональных данных, контроля субъекта данных, ответственности распорядителя данных и обеспечения безопасности данных;*
- *разработки национальных стратегий с целью координирования усилий всех акторов на государственном уровне и активизации сотрудничества между уполномоченными органами по защите персональных данных;*
- *подотчётности оператора (распорядителя, контролера) данных независимо от местонахождения данных, а также независимо от того, обрабатываются ли данные самим оператором, его представителями или передаются другому оператору.*

В ходе подготовки законодательства о защите персональных данных необходимо проводить его общественное обсуждение, поскольку оно затрагивает гражданские свободы в онлайн-среде. Защита персональных данных должна быть темой кампании по информированию общественности, направленной на совместное обсуждение вопроса гражданами, правозащитными группами, коммерческими компаниями и государственными органами.

Правовая база защиты персональных данных не должна проводить различие между частным и государственным секторами. Граждане просто не поймут такое различие

в условиях, когда государственный сектор собирает, сопоставляет, а иногда даже хочет продавать персональные данные.

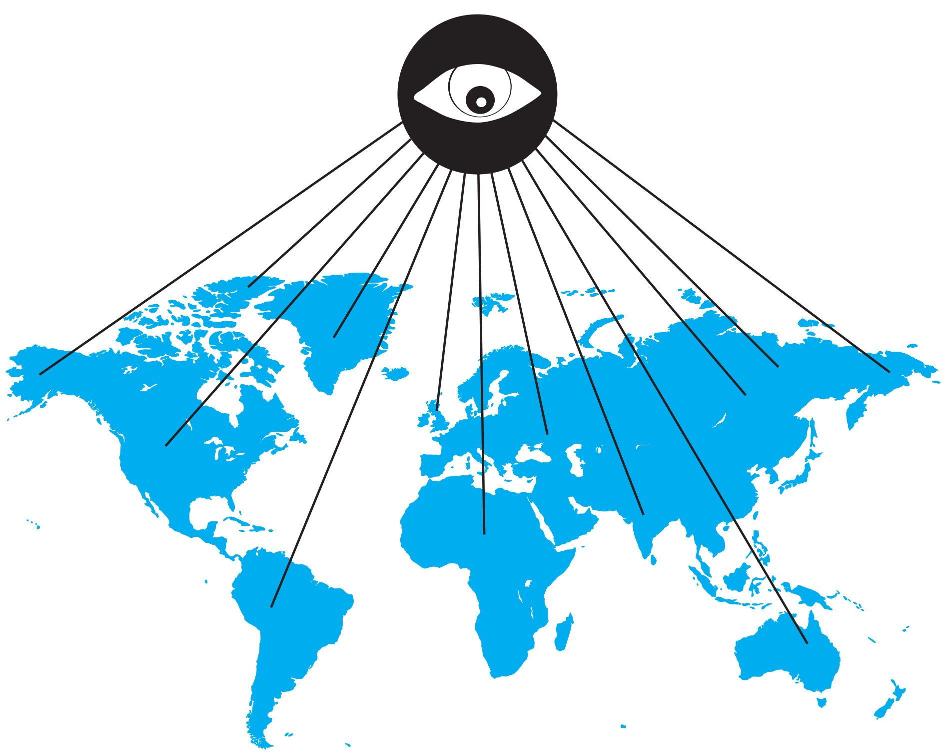
Исключения со ссылкой на интересы национальной безопасности должны использоваться экономно. Они должны быть именно исключениями, а не правилом. Необходимость защиты национальной безопасности может оправдать особые нормы. Однако не все, что относится к внешним связям, является вопросами национальной безопасности. Иной подход подрывает легитимность законов, имеющих жизненно важное значение для нашей безопасности.

В сфере защиты персональных данных надзора со стороны исполнительной власти недостаточно. Необходим парламентский и судебный контроль.

Правозащитники и гражданские активисты, наряду с представителями государственных органов и бизнеса, могут и должны быть активными участниками диалога о стратегиях, приоритетах и балансе в сфере защиты персональных данных.

Раздел 3.

ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ



МЕЖДУНАРОДНЫЕ ПРИНЦИПЫ И СТАНДАРТЫ

Как отмечалось в предыдущих главах, уже в 1960-х гг. стало очевидным, что проблемы защиты индивида в связи с автоматизированной обработкой и передачей персональных данных не могут быть решены при помощи только лишь национальных средств правовой защиты персональных данных. Попытки правового регулирования трансграничных потоков данных посредством национальных законов были либо недостаточно эффективны, либо приводили к фактическому запрету на экспорт данных.

Защита данных не похожа на охрану окружающей среды, где государства могут договориться о желаемом уровне токсинов и при этом иметь относительное четкое взаимное представление об этом уровне. Защита данных требует более целостного подхода, предполагающего участие в совместной работе широкого круга действующих лиц – обработчиков данных, субъектов данных, регулирующих органов. Здесь требуется совместный процесс обучения и посредничества снизу вверх, равно как и меры регулирования и принудительного исполнения сверху вниз[1]

Защита данных не похожа на охрану окружающей среды, где государства могут договориться о желаемом уровне токсинов и при этом иметь относительное четкое взаимное представление об этом уровне. Защита данных требует более целостного подхода, предполагающего участие в совместной работе широкого круга действующих лиц – обработчиков данных, субъектов данных, регулирующих органов. Здесь требуется совместный процесс обучения и посредничества снизу вверх, равно как и меры регулирования и принудительного исполнения сверху вниз[2].

Глобальное информационное пространство, сформировавшееся в результате реализации таких инициатив, можно представить, как группу «островов», каждый из которых символизирует собой сообщество стран, гармонизировавших свое законодательство о защите данных под эгидой конкретной международной организации (ОЭСР, Совета Европы, Евросоюза, ОАГ). Эти «острова» гармонизированного законодательства окружены «морем» стран, не располагающих адекватным (по критериям международных организаций) или вообще каким-либо законодательством о защите персональных данных. Внутри каждого сообщества стран, гармонизировавших свое законодательство по определённым критериям осуществляется свободный трансграничный обмен персональными данными. Вектор дальнейшего развития информационного пространства в рамках таких сообществ - создание интегрированной информационной инфраструктуры на базе концепции «информационных магистралей» (information highway), одним из главных аспектов которого является формирование единообразного законодательства в рамках данного сообщества стран.

Ключевой проблемой международного правового регулирования обработки и передачи персональных данных с самого начала стала необходимость достижения консенсуса относительно фундаментальных принципов, на которых должна была

1 Bennett, C.(1998) Application of a Methodology designed to Assess the Adequacy of the Level of Protection of Individuals with regard to Processing Personal Data: Test of the Method on Several Categories of Transfer. European Commission Tender No. XV/97/18/D, September 1998. Доступно через: http://ec.europa.eu/justice/data-protection/document/studies/files/19980901_adequacy_methodology_en.pdf.

2 Там же.

основываться защита данных. Без достижения такого консенсуса невозможно разрешение конфликта законодательств разных стран при трансграничной передаче данных.

Поскольку не существовало никакой международной организации, которая могла бы установить единые «правила игры», инициативу взяли на себя транснациональные организации, представляющие политико-экономические союзы и сообщества государств: ООН, ОЭСР, Совет Европы, Европейский союз.

ООН

В резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (ноябрь, 1999 г.) отмечается необходимость разработки международных принципов, которые были бы направлены на усиление безопасности глобальных информационных и телекоммуникационных систем и способствовали борьбе с информационным терроризмом и криминалом[1].

В настоящее время высказываются предложения о том, что органом, обеспечивающим надлежащую защиту прав субъектов персональных данных на глобальном уровне может стать межправительственное объединение – Организация Объединенных Наций[2].

ОЭСР

Поскольку национальные системы правовой защиты данных не смогли обеспечить экстерриториальность персональных данных, а существующая «разноголосица законов» препятствовала созданию международной системы правового регулирования обработки персональных данных, то в 1978 г. ОЭСР обратилась к проблеме дивергенции национальных законов в этой области. Была учреждена специальная экспертная группа с задачей разработать набор базовых руководящих принципов защиты приватности в связи с обработкой персональных данных и в связи с трансграничными потоками данных. Эти принципы должны были послужить основой для гармонизации соответствующих национальных законов.

Разработка принципов и достижение консенсуса стран-участниц оказались непростой задачей, поскольку весьма неоднородный состав ОЭСР предопределил не менее неоднородный набор национальных подходов к правовой защите персональных данных. Так, например, некоторые национальные законы защищали как данные физических лиц, так и «персональные данные», относящиеся к юридическим лицам. В рамках одних юрисдикций термин «персональные данные» относился только к данным, подвергающимся автоматической обработке, а в других – и к рукописным, и печатным сведениям. Разнились и подходы к построению национальной системы

1 Генеральная Ассамблея ООН (1999) Резолюция A/RES/54/49 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Доступно через: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N99/777/15/PDF/N9977715.pdf?OpenElement.

2 Hert, P. (2013) Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency? Доступно через: http://moritzlaw.osu.edu/students/groups/is/files/2013/08/7-Hert-Papakonstantinou.pdf

правовой защиты персональных данных. В одних странах существовал один основной закон защиты персональных данных, в других предпочтение отдавалось секторальному регулированию, в-третьих действовал как основной закон о защите персональных данных, так и отраслевые нормы.

По итогам двухлетней работы экспертной группы, включая процесс согласования разрабатываемых принципов со всеми странами-участницами, Совет ОЭСР принял «Рекомендации в отношении Руководящих принципов по защите неприкосновенности частной жизни и трансграничных потоков персональных данных». Руководящие принципы были оформлены как приложение к рекомендациям Совета и сопровождались специальным Пояснительным меморандумом, разъяснявшим причины, лежащие в основе их формулировок.

В документе констатируется, что Руководящие принципы разработаны с целью:

а) достижения странами-участницами определенных минимальных стандартов защиты приватности и прав субъектов персональных данных;

б) уменьшения различий между релевантными отечественными нормативными положениями конкретной страны и практикой других стран-участниц;

в) гарантии того, что при защите персональных данных на национальном уровне будут учитываться негативные последствия ненадлежащего вмешательства в потоки персональных данных между государствами-членами ОЭСР;

г) устранения причин, которые могли бы побудить государства ограничивать или запрещать трансграничные потоки персональных данных из-за возможных рисков, ассоциируемых с такими потоками.

Руководящие принципы ОЭСР состоят из пяти частей:

1. определения и сфера действия документа;
2. принципы защиты приватности и индивидуальных свобод в связи с обработкой персональных данных на национальном уровне;
3. принципы международного применения, которые относятся, главным образом, к взаимодействию между странами-членами ОЭСР;
4. меры по осуществлению на практике вышеупомянутых базовых принципов;
5. организация взаимодействия и сотрудничества стран-членов ОЭСР (главным образом, посредством обмена информации и избежание несовместимых национальных процедур для защиты персональных данных).

Международно- признаваемые принципы впервые были формально зафиксированы европейской организацией ОЭСР (Организация экономического сотрудничества и развития) в 1980 г., в целях защиты прав субъектов данных и определения ответственности пользователей данных.

Признаваемые на международном уровне принципы впервые были формально зафиксированы ОЭСР (Организацией экономического сотрудничества и развития) в 1980 г. в целях защиты прав субъектов данных и определения ответственности пользователей данных. Эти принципы до сих пор лежат в основе формирования политики и разработки правовых инструментов защиты персональных данных.

1. Руководящие принципы защиты персональных данных ОЭСР:
2. ограничение сбора. Данные должны быть получены законным и честным путем и, где это возможно, с ведома или согласия субъекта данных;

3. качество данных. Персональные данные должны соответствовать целям, для которых они должны быть использованы, и в этом отношении должны быть точны, полны и актуальны;

4. определение цели. Цели, для которых собираются персональные данные, должны быть определены не позднее времени сбора данных, а последующее использование данных ограничивается соответствием этим целям или другим целям, не являющимся несовместимыми с этими целями, и подобное определение происходит в каждом случае изменения целей;

5. ограничения использования. Персональные данные не должны раскрываться, делаться доступными или другим образом использоваться в целях, не определенных в соответствии с параграфом 9 (принцип определения цели), за исключением а) с согласия субъекта данных или б) в соответствии с законом;

6. средства безопасности. Персональные данные должны быть защищены разумными средствами безопасности от таких рисков, как потеря или несанкционированный доступ, уничтожение, использование, модификация или раскрытие данных;

7. открытость. Должна проводиться общая политика открытости в отношении разработок, практик и политики в сфере персональных данных. Должны быть всегда доступны средства и способы для установления наличия и характера/типа персональных данных, главной цели их использования, также, как и их подлинности, а также обычного местонахождения контролера данных;

8. Участие индивидов (субъектов данных). Индивид должен иметь право:

   a. получать от контролера данных, или иным образом, подтверждение, имеет ли контролер данных данные, относящиеся к нему;

   b. при общении с индивидом, данные относящиеся к нему, должны быть предоставлены:

      - в разумное время;
      - за доступную плату, если а такая установлена;
      - разумным способом; и
      - в форме, действительно доступной им для понимания;

   c. узнавать причины в случае отклонения запросов по подпараграфам (а) или (b), и иметь возможность оспорить такое отклонение запросов; и

   d. оспаривать данные, относящиеся к инивидуму, и если это возможно, обеспечить стирание, очистку, завершение или актуализацию данных;

9. подотчетность. Контролер данных должен быть подотчетен в отношении соблюдения мер, позволяющих работать согласно вышеприведенным принципам[1].

Эксперты ОЭСР сформулировали также подходы к двум принципиальным проблемам, остающимся актуальными до настоящего времени:

- *право на приватность для юридических лиц;*

1 Энн Кавукян, помощник комиссионера по прайвеси штата Онтарио. Доступно через: http://privacy-ru.livejournal.com/852.html.

- *соотношение регулирования автоматизированной и неавтоматизированной обработки данных.*

Корпоративная приватность. Некоторые члены экспертной группы предполагали, что должна быть предусмотрена возможность распространения Руководящих принципов на юридических лиц (корпорации, ассоциации и т.п.). Однако это предложение не получило одобрения большинства членов группы. В итоговом варианте Руководящих принципов ОЭСР отмечается: неприкосновенность личности и частной сферы индивидуума является во многих аспектах особенной и не должна трактоваться тем же самым образом, что и неприкосновенность некой группы физических лиц или корпоративная безопасность и конфиденциальность. Потребности в защите у этих двух категорий совершенно различны. Государства-члены ОЭСР должны принять решения относительно национальной политики по отношению к приватности корпораций, групп, партий и иных подобных организаций.

Автоматизированные и неавтоматизированные персональные данные. Экспертная группа пришла к заключению, что ограничение Руководящих принципов только областью автоматизированной обработки персональных данных было бы существенным недостатком, поскольку:

10. трудно провести различие между автоматизированной и неавтоматизированной обработкой данных при наличии смешанных систем обработки данных и таких стадий в обработке данных, которые могут привести к автоматизированной обработке, а могут и не привести;
11. сужение сферы принципов регулирования могло бы привести к непоследовательности и лакунам, предоставить контролерам данных удобную возможность для обхода общих правил и национальных законов, реализующих на практике эти Руководящие принципы при помощи использования неавтоматических средств для определенных целей. Именно в силу вышеуказанных трудностей.

Вот почему Руководящие принципы не устанавливают определения «автоматизированной обработки данных», хотя само это понятие упоминается в преамбуле и в § 3. А принципы защиты прав субъектов персональных данных распространяются на обработку данных вообще, безотносительно к конкретной используемой технологии.

Иными словами, Руководящие принципы ОЭСР применяются к персональным данным, обработанным таким способом, который представляет собой опасность для права неприкосновенности частной жизни и индивидуальных свобод в силу характера или контекста этих данных.

Вместе с тем, принципы не относятся к вмешательству в сферу частной жизни. Несанкционированная фотосъемка, тайное наблюдение или диффамация находятся вне сферы их действия, если только такие деяния не связаны с обработкой персональных данных. Руководящие принципы посвящены исключительно вопросам создания и использования агрегатов данных (т.е. файлов, банков данных, досье, публикаций, документов и т.п.), которые специально организованы для хранения и последующего воспроизведения, публикации, принятия решений, проведения исследований и других подобных целей[1].

В Руководящих принципах отсутствуют положения, касающиеся «уязвимых данных», поскольку в странах-членах ОЭСР существуют серьезные расхождения в трактовке таких данных.

Руководящие принципы ОЭСР нейтральны по отношению к используемой технологии;

1 OECD documents. Privacy and data protection: Issues and Challenges, Information Computer Communication Policy. OECD Paris, 1966.

применяются к персональным данным, обработанным таким способом, который представляет собой опасность для права неприкосновенности частной жизни и индивидуальных свобод в силу характера или контекста этих данных;

относятся исключительно к созданию и использования агрегатов данных (т.е. файлов, банков данных, досье, публикаций, документов и т.п.), которые специально организованы для хранения и последующего воспроизведения, публикации, принятия решений, проведения исследований и других подобных целей.

Несмотря на юридически не обязательный характер, Руководящие принципы оказали большое влияние на становление национальных систем правовой защиты субъектов персональных данных, причем, не только в странах ОЭСР.

В 1985 г. за ними последовала Декларация о трансграничных потоках данных, а в 1998 г. была опубликована Министерская декларация об охране неприкосновенности личной жизни в глобальных сетях, в которой было снова заявлено о необходимости единых подходов к проблеме трансграничных потоков данных и охраны неприкосновенности личной жизни в глобальных сетях. В более недавний период, в 2007 г., Совет ОЭСР принял новую Рекомендацию ОЭСР, касающуюся трансграничного сотрудничества в вопросе принудительного исполнения законов, охраняющих неприкосновенность личной жизни. Документ преследует целью оказание взаимопомощи при исполнении законов о неприкосновенности личной жизни. Ожидается, что он окажет влияние на взаимодействие на глобальном уровне.

В июне 2008 г. в Сеуле, Южная Корея, ОЭСР провело министерское совещание на тему «Будущее интернет-экономики». На совещании генеральный секретарь ОЭСР высказался в поддержку усилий по приданию официального статуса участию гражданского общества и экспертов в области интернет-технологий в работе ОЭСР, посвященной будущему сети интернет[1]. В марте 2009 г. ОЭСР официально оформила участие в своей работе представителей гражданского общества и технических экспертов, присоединив их к представителям профсоюзов и частного сектора, которые работают на основе принципа многостороннего сотрудничества через один из комитетов организации.

Пересмотр руководящих принципов обусловлен принятием Сеульской декларации о будущем интернет-экономики. В Сеульской декларации, в которой содержится призыв к ОЭСР провести оценку применения определенных правовых документов, в том числе и руководящих принципов в области неприкосновенности личной жизни, в свете «меняющихся технологий, рынков, моделей поведения пользователей и растущей значимости цифровых способов установления личности». Исходя из утвержденного технического задания по пересмотру Руководящих принципов ОЭСР в области неприкосновенности личной жизни можно сделать вывод, что будет проведено изучение изменений реальной ситуации с точки зрения роли личных данных в экономике, обществе и жизни людей[2]. В настоящее время данный процесс находится в стадии обсуждения.

1 Gurría, A (2008) Message from OECD Secretary-General. Доступно через: http://www.oecd.org/forum/50485127.pdf.

2 OECD (2011) Thirty years after. The OECD privacy guidelines. Доступно через: http://www.oecd.org/sti/ieconomy/49710223.pdf.

СОВЕТ ЕВРОПЫ

В 1950 г. Совет Европы принял Европейскую конвенцию о защите прав человека и основных свобод (ЕКПЧ). В статье 8 «Право на уважение частной и семейной жизни» ЕКПЧ неприкосновенность личной жизни сформулирована следующим образом:

> *Каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции.*
>
> *Не допускается вмешательство со стороны публичных властей в осуществление этого права, за исключением случаев, когда такое вмешательство предусмотрено законом и необходимо в демократическом обществе в интересах национальной безопасности и общественного порядка, экономического благосостояния страны, в целях предотвращения беспорядков или преступлений, для охраны здоровья или нравственности, или защиты прав и свобод других лиц.*

В рамках судебной практики учрежденного в соответствии с ЕКПЧ Европейского суда по правам человека право на неприкосновенность личной жизни, закрепленное статьей 8, получило широкое толкование.

В 1968 г. Парламентская ассамблея Совета Европы обратилась к Комитету министров с Рекомендацией 509, с просьбой рассмотреть вопрос о том, предоставляет ли Европейская конвенция о защите прав человека и внутреннее право государств-членов достаточную защиту права на частную жизнь в связи с развитием современной науки и технологии. Исследования, проведенные по указанию Комитета министров в качестве ответа на данную Рекомендацию, показали, что в настоящее время национальное законодательство в странах не обеспечивает достаточной защиты частной жизни людей и других прав и интересов физических лиц в отношении автоматизированных банков данных.

Исходя из этих выводов Комитет министров принял в 1973 и 1974 гг. две резолюции о защите данных. В первой Резолюции (73) 22 устанавливаются принципы защиты данных в частном секторе, а во второй Резолюции (74) 29 - для общественного сектора.

Вскоре, однако, стало очевидно, что ввиду различной трактовки концепции «приватности» в разных странах экстерриториальная защита персональных данных невозможна без общих принципов защиты данных, которые позволили бы гармонизировать национальные законы стран-участниц. Парламентская ассамблея Совета Европы, принимая во внимание эту тенденцию, рекомендовала Комитету министров в своей Рекомендации 890 (1980) изучить возможность включения в Конвенцию о защите прав человека положения о защите личных данных.

После четырех лет переговоров, страны-члены Совета Европы в 1981 г. приняли Конвенцию № 108 Совета Европы (Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера).

Это первый обязательный для исполнения международный специальный договор, посвященный охране персональных данных. В нем определен ряд главных принципов, в дальнейшем положенных в основу многих законов о неприкосновенности личной жизни. Конвенция также защищает физических лиц от вторжения в их личную жизнь со стороны государственных органов и администрации частных организаций. Ратификация конвенции осуществляется в добровольном порядке, но после ратификации она становится юридически обязывающим документом на национальном уровне. На сегодняшний день конвенция ратифицирована 44 странами. Она

открыта для подписания странами, входящими и не входящими в состав членов Совета Европы[1].

Цель Конвенции Совета Европы –в достижении большего единства между его членами, основанного, в частности, на уважении принципа верховенства права, а также соблюдении прав человека и основных свобод. Положения Конвенции разработаны с учетом:

необходимости усиления защиты прав и основных свобод каждого человека, и в частности права на уважение частной жизни;

увеличения трансграничного потока персональных данных, подвергающихся автоматизированной обработке;

обеспечения свободы распространения информации между народами, невзирая на границы.

По условиям Конвенции 108 подписавшие и ратифицировавшие ее стороны обязывались принять (или скорректировать) национальные законы таким образом, чтобы они обеспечивали соблюдение на практике изложенных в этой Конвенции базовых принципов в отношении защиты прав субъектов персональных данных при автоматической обработке таких данных.

Конвенция состоит из трех главных частей:

- *положения материального права в форме основных принципов;*
- *специальные нормы в отношении трансграничных потоков данных;*
- *механизмы для оказания взаимной помощи и проведения консультаций между сторонами.*

Главной отправной идеей Конвенции является то, что некоторые права физических лиц могут нуждаться в защите в контексте свободного трансграничного потока информации ниц, и этот принцип закреплен в международных и европейских документах в сфере прав человека (см. статью 10 Конвенция о защите прав человека и основных свобод; статью 19 Международного пакта о гражданских и политических правах).

Ограничения свободы информации, в соответствии с Конвенцией, возможны только с целью защиты других индивидуальных прав и свобод, в частности права на неприкосновенность частной жизни (см. статью 8 Конвенция о защите прав человека и основных свобод).

Основная часть Конвенции – Глава II, в которой излагаются основополагающие принципы защиты данных (эти положения исходят из ранее закрепленных принципов в Резолюциях (73) 22 и (74) 29 Комитета министров, а там, где необходимо, эти принципы дополнены с учетом последующего развития законодательства в государствах-членах)[2].

В соответствии с Конвенцией, защита данных включает: (а) принципы качества данных; (б) права субъекта данных. Они устанавливаются соответственно в ст. 5 и 8. Все персональные данные, подлежащие обработке, должны быть защищены соответствующими мерами безопасности (ст. 7).

1 Greenleaf, G.(2011) Global Data Privacy in a NetworkedWorld. Доступно через: http://ssrn.com/abstract=1954296.

2 Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера. Пояснительный доклад. Доступно через: http://www.conventions.coe.int/Treaty/rus/Reports/Html/108.htm.

Ст. 6 Конвенции вводит понятие специальных категорий данных (персональные данные, касающиеся расовой принадлежности, политических взглядов или религиозных, или других убеждений, а также персональные данные, касающиеся здоровья или половой жизни, данные о судимостях), которые «не могут подвергаться автоматизированной обработке, если внутреннее законодательство не устанавливает соответствующих гарантий». Допускается расширение перечня «особо чувствительных» персональных данных в национальных законодательствах стран-участниц Конвенции, но не обратное.

Конвенция постулирует, что трансграничная передача данных может быть ограничена, если:

1. защита персональных данных в стране-контрагенте не является «адекватной» (ст. 12);
2. данные, передаваемые на территорию страны-контрагента, предназначены для передачи транзитом в некую третью страну, не являющуюся участницей Конвенции.

Для обеспечения взаимного сотрудничества и содействия страны-участницы Конвенции обязаны учредить национальный орган (или органы) по защите данных, к которому можно было бы обращаться за помощью и содействием (ст. 13). Консультативный комитет, состоящий из делегатов от государств, подписавших Конвенцию, отвечает за толкование положений Конвенции и за содействие и улучшение их применения на практике (ст. 18-20).

В 1992 г. Консультативный комитет по Конвенции 108 принял набор типовых договорных положений, которые должны обеспечить защиту персональных данных, а также передаваться публичной или частной организацией из страны, ратифицировавшей Конвенцию 108, в страны, которые не приняли меры, обеспечивающие адекватную защиту.

В 2001 г. был принят Дополнительный протокол к 108-й Конвенции Совета Европы, который предусматривает:

- *учреждение национального надзорного органа, который обязан следить за соблюдением законодательства в области защиты данных и требовать от не присоединившихся к Конвенции стран-получателей данных обеспечения адекватного уровня их защиты;*
- *требование ко всем странам-членам СЕ предоставить надзорным органам полную независимость;*
- *право участников Конвенции принимать законодательные меры по ограничению потоков данных в не присоединившиеся к Конвенции страны и ожидать аналогичного уровня защиты от страны-участника конвенции в отношении определенных категорий уязвимых данных*.

В ходе подготовки проекта тема трансграничного потока данных вызвала жаркую дискуссию. Комитет, отвечавший за подготовку проекта, рассматривал два варианта международных договоренностей. Первый из них предусматривал взаимность: страна должна была запретить обработку данных на своей территории, если в другой стране она считалась незаконной, а данные касались жителей и граждан этой другой страны. Предпочтение было отдано второму варианту – установлению в качестве стандарта общего свода принципов защиты данных. В 2009 г. коалиция в составе более 100 различных групп подготовила Мадридскую декларацию о неприкосновенности личной жизни, в которой содержится призыв к установлению общемировых стандартов в области неприкосновенности личной жизни.

Как и предполагалось в самой Конвенции 108, институты Совета Европы продолжают работать над различными аспектами правового регулирования защиты персональных данных на региональном уровне. Результаты этой работы представляются в форме рекомендаций, резолюций и деклараций.

Таким образом система инициатив Совета Европы в области защиты персональных данных имеет иерархический характер:

- *«базовая» инициатива - Конвенция 108;*
- *секторные инициативы – рекомендации Совета Европы.*

Механизм разработки и принятия рекомендаций по защите персональных данных. Комитет министров в 1976 г. учредил специальную проектную группу по защите данных, которая состоит из высокопоставленных должностных лиц от всех стран-членов Совета Европы, ответственных за защиту персональных данных в своих странах. Для разработки специфических отраслевых (секторных) рекомендаций эти официальные лица часто имеют советников из соответствующих отраслей и секторов национальной экономики. Проектная группа контролирует инициативы в области защиты данных и часто просит Консультативный комитет, действующий согласно положениям Конвенции 108, исследовать конкретные темы, вызывающие озабоченность в связи с защитой персональных данных.

Работа проектной группы по большей части выполняется в специализированных рабочих подгруппах, сложившихся за последнее десятилетие. Охват широкого спектра мнений обеспечивается тем, что в общих собраниях проектной группы (они проводятся каждые полгода) и в деятельности Консультативного комитета могут участвовать (разумеется, без права участия в голосовании) представители Европейского союза (ЕС), Международной торговой палаты, международных профессиональных и потребительских организаций и наблюдатели от стран, не ратифицировавших Конвенцию 108. Предложения проектной группы часто рассматриваются европейским Комитетом по законодательному сотрудничеству прежде, чем Комитет министров вотирует их. Иногда эти предложения также подлежат рассмотрению Руководящей комиссией по правам человека, которая несет общую ответственность за координацию работы Совета Европы, связанной с европейской Конвенцией о правах человека. Эта комиссия, например, рассматривала проект рекомендаций по защите данных в области телекоммуникационных услуг.

Рекомендации имеют преимущество по отношению к директивам, поскольку их легче тщательно проработать в деталях. Для введения рекомендаций в действие необходимо только единогласное принятие их Комитетом министров (таким образом, нет необходимости в длительном процессе подписания и ратификации каждой страной). Хотя рекомендации не являются юридически обязывающими, они адресуются всем странам-членам Совета Европы (независимо от того, является ли данная страна участницей Конвенции 108 или нет), которые наделены моральным обязательством добросовестно принимать во внимание эти рекомендации. Рекомендации конкретизируют основополагающие принципы Конвенции 108 и адаптируют их к изменяющимся социально-политическим и технологическим контекстам.

К настоящему времени Комитет министров принял следующие Рекомендации в рамках реализации Конвенции 108:

- *Рекомендация № R(81) 1 (от 23 января 1981 г.) об общих правилах для автоматизированных банков медицинских данных (в настоящее время пересматривается);*
- *Рекомендация № R(83) 10 (от 23 сентября 1983 г.) о персональных данных, используемых для научных исследований и статистики (в настоящее время пересматривается);*

- *Рекомендация № R(86) 1 (от 23 января 1986 г.) о персональных данных, используемых для целей социального обеспечения:*
- *Рекомендация № R(87) 15 (от 17 сентября 1987 г.). регламентирующая использование персональных данных полицейскими властями;*
- *Рекомендация № R(89) 2 (от 18 января 1989 г.) о защите персональных данных, используемых в целях трудоустройства;*
- *Рекомендация № R(90) 19 (от 13 сентября 1990 г.) о защите персональных данных, используемых для платежей и связанных с ними операций;*
- *Рекомендация № R(91) 10 (от 9 сентября 1991 г.) о сообщении третьим сторонам персональных данных, хранимых общественными организациями;*
- *Рекомендация № R(95) 4 о защите персональных данных в области телекоммуникационных услуг, с конкретными ссылками на телефонные услуги;*
- *Рекомендация № R(12)4 о защите прав человека в отношении социальных сетевых сервисов;*
- *Рекомендация № R(12) 3 о защите прав человека в отношении в отношении поисковых систем;*
- *Рекомендация № R(10) 13 о защите индивидов в отношении автоматической обработки данных в контексте профилирования (объединения данных);*
- *Рекомендация № R(02) 9 о защите персональных данных, собираемых и обрабатываемых в целях страхования;*
- *Рекомендация № R(99) 5 о защите приватности в интернете;*
- *Рекомендация № R(97) 18 о защите персональных данных, собираемых и обрабатываемых в статических целях;*
- *Рекомендация № R(97) 5 о защите медицинских данных и ряд других документов[1].*

В 2013 г. была опубликована Декларация Совета министров об опасностях трекирования и цифровой слежки[2].

Заложенные Конвенцией принципы в целом не привязаны к той или иной технологии и благодаря этому с течением времени продолжают сохранять свое действие. Однако в марте 2010 г. Комитет министров Совета Европы одобрил идею актуализации 108-й конвенции и призвал к укреплению механизма наблюдения за реализацией ее положений[3].

Хотя обсуждения, в основном, сосредоточены вокруг самой 108-й конвенции, министры в настоящее время рассматривают вопрос дальнейшего развития действующих принципов защиты данных с приведением их в соответствие с текущими реалиями, уровнем технологического развития и эффективным механизмом реализации[4]. Данный процесс пока не завершен.

1 Data protection. Legal instruments. Доступно через: http://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp.
2 http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/Decl_Digital_tracking_EN_11%2006%202013E.pdf.
3 DP (2010) textes. Data protection. Compilation of Council of Europe texts. Доступно через: http://www.coe.int/t/dghl/standardsetting/dataprotection/dataprotcompil_en.pdf.
4 Там же.

ЕВРОПЕЙСКИЙ СОЮЗ

Регулирование защиты персональных данных (качество данных и права субъектов данных) осуществляется в рамках трех базовых документов: Договора ЕС, Договора о функционировании ЕС и Хартии ЕС о правах человека.

Регулирование защиты персональных данных (качество данных и права субъектов данных) осуществляется в рамках Договора ЕС, Договора о функционировании ЕС и Хартии ЕС о правах человека.

Договор о ЕС, статья 39

В соответствии со статьей 16 Договора о функционировании Европейского союза и в отступление от параграфа 2 статьи Совет принимает решение, устанавливающее правила о защите физических лиц в отношении обработки персональных данных государствами-членами при осуществлении деятельности, которая входит в сферу применения настоящей главы, и о свободном перемещении таких данных. Соблюдение этих правил находится под контролем независимых органов.

Договор о функционировании ЕС, статья 16

1. Каждый имеет право на защиту относящихся к нему персональных данных.

2. Европейский парламент и Совет, постановляя в соответствии с обычной законодательной процедурой, устанавливают правила о защите физических лиц в отношении обработки персональных данных институтами, органами и учреждениями Союза, а также государствами-членами при осуществлении деятельности, которая входит в сферу применения права Союза, и о свободном перемещении таких данных. Соблюдение этих правил находится под контролем независимых органов.

Правила, принимаемые на основании настоящей статьи, не наносят ущерба специальным правилам, предусмотренным в статье 39 Договора о Европейском союзе.

Хартия ЕС по правам человека содержит следующие положения о защите персональных (личных) данных:

Статья 7: Уважение личной и семейной жизни

Каждый имеет право на уважение своей личной и семейной жизни, жилища и общения.

Статья 8: Защита личных данных

Каждый имеет право на защиту касающихся его личных данных.

1. *Такие данные должны обрабатываться должным образом в указанных целях на основании согласия затрагиваемого лица либо на иных законных основаниях, установленных законом.*

2. *Каждый имеет право доступа к данным, которые были собраны в его отношении, а также право на обеспечение их исправления.*

3. *Соблюдение данных правил подлежит контролю со стороны независимого органа.*

В 1990 г. Совет Европейского союза принял решение о разработке проектов двух директив:

- *«базовой» директивы о защите частных лиц по отношению к обработке персональных данных, определяющей общую регламентацию защиты данных;*
- *«отраслевой» директивы о защите приватности и персональных данных при передаче данных с использованием цифровых телекоммуникационных сетей связи общего пользования, в частности, работающих на базе протокола связи ISDN, и по каналам цифровых сетей мобильной связи общественного пользования.*

В процессе согласования проектов выявились серьезные разногласия между странами-членами ЕС относительно степени строгости правила получения «согласия субъекта данных» и передачи персональных данных по телекоммуникационным линиям в третьи страны.

Окончательный текст «базовой» директивы был опубликован в 1995 г., а в 1996 г. была опубликована секторальная директива – о защите персональных данных. Директива 1996 г. утратила силу после принятия Директивы Европейского парламента и Совета Европейского союза 2002/58/ЕС от 12 июля 2002 г. в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи)[1]. В этом же году была принята Директива Европейского парламента и Совета Европейского союза 2002/22/ЕС от 7 марта 2002 г. об универсальных услугах и правах пользователей в отношении сетей электронных коммуникаций и услуг (Директива об универсальных услугах).

Непосредственно защиту качества данных и права субъектов персональных данных регулирует Директива № 95/46/ЕС Европейского парламента и Совета Европейского Союза о защите физических лиц при обработке персональных данных и о свободном обращении таких данных[2].

Директива ЕС о неприкосновенности личной жизни и об электронных коммуникациях 2002/58/ЕС – установила конкретные требования, касающиеся сети интернет, затронув такие чувствительные темы, как сохранение данных, электронные сообщения, направляемые «без спроса», использование фрагментов данных типа cookies, а также включение личных данных в каталоги для общего пользования.

Общие принципы, заложенные в европейскую Директиву о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, аналогичны принципам 108-й Конвенции Совет Европы и «Руководящим принципам» ОЭСР. Новаторской нормой, по сравнению с Конвенцией 108 и Руководящими принципами ОЭСР, стала статья 15, которая касается «автоматических решений физического лица» и призвана решить проблему практики формирования профилей пользователей

Общие принципы, заложенные в европейскую директиву, аналогичны принципам 108-й Конвенции Совета Европы и Руководящим принципам ОЭСР. Требования директивы распространяются на все типы обработки данных за исключением операций, касающихся общественной безопасности, обороны и государственной безопасности.

1 Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. Международное законодательство. Доступно через: http://pd.rkn.gov.ru/law/.

2 Директива Европейского парламента и Совета Европейского союза 95/46/ЕС от 24 октября 1995 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных (в редакции Регламента Европейского парламента и Совета ЕС 1882/2003 от 29 сентября 2003 года). Доступно через: http://pd.rkn.gov.ru/docs/Direktiva_Evropejskogo_Parlamenta_i_Soveta_Evropejskogo_Sojuz_95_46_ES.rtf.

Директива предусматривает высокий уровень защиты данных, устанавливая строгие ограничения в отношении сбора, использования и раскрытия личных данных. Соблюдение требований в каждой стране ЕС должен обеспечивать независимый национальный орган с надзорными полномочиями. Согласно требованиям директивы, учреждается консультативная рабочая группа по единообразию применяемых национальных мер, а также мер по защите данных в третьих странах, поскольку трансграничная передача данных в страны за пределами ЕС разрешена только при обеспечении страной-получателем адекватного уровня защиты.

Новаторской нормой, по сравнению с Конвенцией 108 и Руководящими принципами ОЭСР, стала статья 15, которая касается «автоматических решений физического лица» и призвана решить проблему практики формирования профилей пользователей[1].

Директивы, в отличие от Конвенции, имеют обязательную юридическую силу для всех стран-членов ЕС, которые обязаны их исполнять в качестве рамочного законодательного акта, подлежащего включению в национальное законодательство. Это требование обеспечило единообразное отношение к обработке личных данных на всей территории ЕС. Кроме того, за счет наличия требований к трансграничным потокам данных директива представляет собой документ, оказывающий значительное влияние на другие страны мира.

Директива 1995 г. включает жесткие требования по отношению к коммерческим предприятиям (хозяйствующим субъектам). Вследствие этого, директива воспринималась не только как требование законодательного закрепления неприкосновенности частной жизни, но и как угроза свободной торговле на фоне усиления глобализации экономики. В частности, Международная торговая палата отметила следующие негативные последствия введения в действие директивы:

- *высокие затраты на обеспечение соблюдения требований директивы,*
- *препятствия внедрению на рынок новых товаров и услуг,*
- *подрыв стимулов к инвестированию.*

Отношение международного бизнес-сообщества к сбалансированной защите сферы частной жизни и персональных данных индивидуума, с одной стороны, и свободы трансграничных потоков данных, с другой стороны, можно обобщить в 5 базовых принципах, сформулированных в документах Международной торговой палаты:

- *важность защиты приватности частного гражданина, включая защиту против ненадлежащего использования информации, связанной с ним;*
- *важность эффективного обмена информацией в развитии современной международной торговли и коммерции;*
- *право любого бизнеса на свободное общение (свободные коммуникации) как внутри, так и вне его корпоративной структуры;*
- *необходимость признания всемирной зависимости современных бизнес-коммуникаций от трансграничных потоков данных;*
- *необходимость (в тех случаях, когда это приемлемо) гармонизировать средства и меры правовой защиты приватности на международной основе, причем провести эту гармонизацию таким образом, чтобы избежать создания барьеров для международных информационных потоков[2].*

1 Bygrave, L.((2010) Privacy and Data Protection in an International Perspective Доступно через: http://www.uio.no/studier/emner/jus/jus/JUS5630/v13/undervisningsmateriale/privacy-and-data-protection-in-international-perspective.pdf.

2 Protection of Personal Data: An International Business View, Document ICC, No. 373/128, 4 October 1991.

Эти принципы легли в основу обязательных корпоративных правил, рекомендуемых Международной торговой палатой.[1]

В первом отчете о реализации положений директивы 1995 г. Европейская комиссия признала, что избыточные ограничения, особенно вызванные различиями в толковании требования адекватного уровня защиты, оказались «дискредитирующими как саму директиву, так и правовые нормы Сообщества в целом».

В первом отчете о реализации положений директивы 1995 г. Европейская комиссия признала, что избыточные ограничения, особенно вызванные различиями в толковании требования адекватного уровня защиты, оказались «дискредитирующими как саму директиву, так и правовые нормы Сообщества в целом». Тем не менее, ЕК было поручено оценить и определить уровень адекватности, что она и сделала применительно к Норвегии, Лихтенштейну, Исландии, Швейцарии, Канаде, Аргентине, о-ву Гернси, о-ву Мэн и – по отдельному соглашению – США.

Вопреки наличию подробных и достаточно строгих требований к защите данных, а, возможно, и благодаря им, отмечает К. Родригес, данная директива на глобальном уровне оказала существенное влияние на законодательство других стран, при этом не только в Европе. Она послужила в качестве модельного закона для многих стран мира.

Процесс пересмотра директивы ЕС о защите данных

С учетом появления новых технологических разработок – от сайтов социальных сетей и «облачных» методов обработки данных до услуг, привязанных к определенному местоположению пользователя, и смарт-карт – Еврокомиссия начала процесс консультаций по вопросу пересмотра положений Директивы о защите данных 1995 г. От участников процесса, представляющих все группы заинтересованных сторон, поступило несколько предложений[2].

В 2012 г. Европейская комиссия выступила с комплексным предложением по реформированию законодательства в области защиты данных, в том числе с проектом регламента с общими требованиями к защите личных данных физических лиц в процессе их обработки и проектом директивы, посвященной вопросу обработки личных данных в контексте расследования уголовных дел и уголовного преследования.

Следует отметить, что основу предложения составляет проект регламента, а не директивы. Речь идет не просто о смене наименования документа – регламенты «сильнее» директив, поскольку имеют силу закона в странах-членах ЕС и подлежат прямому применению, в то время как положения директив подлежат переносу в национальное законодательство (страны-члены ЕС обязаны принимать законодательные акты, обеспечивающие реализацию поставленных в директиве целей, однако имеют право выбирать способы реализации по собственному усмотрению). Возможно, именно выбор типа нормативно-правового акта в 1995 г. для регулирования системы защиты данных и привел к недостаточной ее гармонизации в силу различ-

1 ICC Task Force on Privacy and Protection of Personal Data (2004) ICC report on binding corporate rules for international transfers of personal data http://www.iccwbo.org/Data/Documents/Digital-Economy/ICC-report-on-Binding-Corporate-Rules/; ICC (2003) Privacy Toolkit . An international business guide for policymakershttp://www.iccwbo.org/privacy_toolkit/.

2 European Commission (2010) Communication from the Commission to the European Parliament, the Council, the Economic and social committee and the Committee of the regions. A comprehensive approach on personal data protection in the European Union. Доступно через: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.

ных способов имплементации в разных странах ЕС. Предложенные Еврокомиссией проекты регламента и директивы до их официального принятия и вступления в силу будут обсуждаться Европейским парламентом и Европейским советом, которые вправе их отклонить и (или) предложить внести изменения.

Требование получения согласия

В статье 7 проекта регламента на контролера данных возложена ответственность за получение согласия субъекта данных на проведение обработки его данных. В статье 4 в определении термина «согласие» подчеркивается, что оно должно носить конкретный и недвусмысленный характер и даваться субъектом данных в виде утверждения или четкого утвердительного действия.

Право «быть забытым»

В статье 17 проекта регламента содержится положение о широко обсуждаемом праве «быть забытым», которое вобрало в себя нормы директивы 1995 года, предусматривающие право физических лиц на удаление своих личных данных после достижения цели, ради которой они обрабатывались и сохранялись. Регламент, однако, пошел дальше, чем директива 1995 года: он предусматривает возможность удаления данных, если такие данные больше не нужны для достижения целей, ради которых они собирались и обрабатывались, или если физическое лицо, которого они касаются, отзывает свое согласие, являвшееся основанием для обработки данных.

Переносимость данных

В проект регламента включено новое право – право на переносимость данных (статья 18), которое позволяет человеку получить свои собственные данные, если они представлены в структурированном и общеупотребительном электронном формате.

Защита данных, гарантированная конструкцией, и защита данных по умолчанию

В соответствии с принципом защиты данных, гарантированной конструкцией, и защиты данных по умолчанию, который содержится в статье 23, компании обязаны учитывать необходимость защиты данных как на самых ранних стадиях разработки продукции, так и в процессе самой обработки данных (защита, гарантированная конструкцией). Хотя данная норма представляет собой шаг в верном направлении, концепция защиты данных должна присутствовать на всех стадиях разработки и выпуска продукции на рынок, а «контролерам данных» должны быть предоставлены определенные стимулы. «Защита данных по умолчанию» означает, что контролер данных должен проследить за тем, чтобы по умолчанию подвергались обработке только те личные данные, которые необходимы для достижения конкретной цели обработки, и чтобы собираемые и сохраняемые данные не превышали пределов необходимости.

Уведомление о нарушении требований безопасности

В проект регламента включено новое обязательство, в соответствии с которым компании должны в течение 24 часов уведомлять национальный надзорный орган о нарушении требований безопасности, касающихся личных данных. Они также обязаны незамедлительно проинформировать о нарушении и физическое лицо, чьих данных оно касается, если существует вероятность того, что нарушение негативно отразится на защите личных данных или на неприкосновенности личной жизни субъекта данных.

Последствия несоблюдения принципов защиты данных

Согласно проекту нового регламента физические лица вправе подавать жалобы в надзорный орган, а также в организации, занимающиеся по поручению физических лиц защитой их прав в области передачи данных. Другими словами, в случае нарушений, предусмотренных проектом регламента прав физических лиц, они имеют право подавать в суд на эти органы и организации, контролера или обработчика личных данных. В проект заложено право на компенсацию, если в результате незаконной операции по обработке данных или иного действия, идущего вразрез с положениями проекта регламента, человеку нанесен ущерб, кроме случаев, когда контролер или обработчик данных доказывают свою непричастность к нанесению ущерба.

Таблица. Ключевые изменения в рамках реформы европейского законодательства вобласти защиты данных[1].

Общий свод правил защиты данных, действующий на всей территории ЕС. Ненужные административные требования, например, обязанность компаний направлять уведомления, будут отменены.
Вместо действующего сегодня требования, обязывающего все компании уведомлять органы по надзору за соблюдением защиты данных обо всех действиях по защите данных, регламентом предусмотрено повышение уровня ответственности и подотчетности лиц, осуществляющих обработку данных.
Компании и организации обязаны в максимально короткий срок (по возможности не позднее 24 часов) уведомлять национальный надзорный орган о серьезных нарушениях требований по защите данных.
Организации будут иметь дело только с одним национальным органом по защите данных в стране ЕС по месту основной регистрации. Аналогичным образом, люди могут обращаться в орган по защите данных в своей стране, даже если обработку их данных осуществляет компания, находящаяся за пределами ЕС. Во всех случаях, когда требуется согласие на обработку данных, четко прописано, что такое согласие необходимо недвусмысленно получить, а не предполагать возможность его получения.
Право «быть забытым» поможет людям более эффективно устранять угрозу защите данных в сети интернет: им будет предоставлена возможность удалять свои данные, если нет законных оснований для их сохранения.
Компании, работающие на рынке ЕС и предлагающие свои услуги гражданам ЕС, будут обязаны при обработке данных за пределами ЕС руководствоваться правилами ЕС.
Независимые национальные органы по защите данных будут усилены, чтобы иметь возможность более эффективно добиваться соблюдения правил ЕС в своих странах. Они будут наделены полномочиями налагать штраф на компании, нарушающие правила ЕС в области защиты данных. Размер штрафных санкций может достигать 1 млн. евро или 2 % суммы годового оборота компании.

Европейский инспектор по защите данных (European Data Protection Supervisor – EDPS) в целом выразил поддержку проектов документов, особенно в части укрепления независимости и национальных органов по защите данных и наделения их полномочиями по принудительному исполнению. При этом он «с сожалением» отмечает «неудовлетворительный характер содержания» директивы о защите данных в сфере правопорядка и юстиции, подчеркивая, что ей недостает жесткости и комплексности. Он согласен с тем, что директива распространяется на обработку дан-

1 European Commission (2012) Proposal for a regulation of the European parliament and of the Council щп the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Доступно через: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

ных внутри ЕС, оговариваясь, что предлагаемый уровень защиты данных по-прежнему слишком низок. По его мнению, Европейская комиссия должна выступить с предложением более строгих правил передачи данных за пределы Евросоюза, а органам по защите данных в обязательном порядке должны быть предоставлены полномочия по организации эффективного контроля над обработкой личных данных в данной сфере[1].

Неправительственная организация «Европейские цифровые права» (European Digital Rights – EDRi) в целом поддержала предложенные реформы. Однако, по мнению экспертов EDRi, нечёткая фиксация права «быть забытым» может повлечь за собой негативные последствия для свободы слова из-за злоупотребления нормой в качестве инструмента цензуры. EDRi также предложила внести ясность в отношении переносимости данных:

- *не возлагать расходы по переносу информации на субъекта данных;*
- *возложить на контролеров и обработчиков данных обязанность предоставлять физическим лицам информацию в общеупотребительном формате*[2].

EDRi также предлагает:

- *в отношении принципа неприкосновенности личной жизни – разработать механизм «эффективной реализации» неприкосновенности личной жизни, гарантированной, например, за счет обязательства проводить оценку обеспечения неприкосновенности личной жизни;*
- *по вопросу уведомлений о нарушении требований по защите данных - создать центральный общедоступный реестр утечек данных;*
- *в отношении предложенной формулировки статьи 42, касающейся мер предосторожности при передаче данных третьим странам, включить требование получения предварительного разрешения у местного надзорного органа*[3].

28 января 2014 года в отмечавшийся в Европе День защиты персональных данных вице-президент Европейской комиссии, Уполномоченный (Еврокомиссар) по вопросам юстиции Вивиан Рединг выступила с речью, в которой сформулировала восемь принципов защиты персональных данных, в соответствии с которыми должна осуществляться обработка персональных данных как в государственном, так и в частном секторах.

Принцип 1: Европа должна создать надежную правовую базу для защиты персональных данных, которая могла бы стать для всего мира образцом и стандартом. В противном случае другие страны нас опередят и навяжут свои стандарты Европе.

Принцип 2: Правовая база защиты персональных данных не должна проводить различие между частным и государственным секторами. Граждане просто не поймут такое различие в условиях, когда государственный сектор собирает, сопоставляет, а иногда даже хочет продавать персональные данные.

Принцип 3: В ходе подготовки законодательства о защите персональных данных необходимо проводить его общественное обсуждение, поскольку оно затрагивает гражданские свободы в онлайн-среде. Защита персональных данных должна быть темой кампании по информированию общественности, направленной на совмест-

1 Opinion of the European Data Protection Supervisor(2012). Доступно через: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-02-20_EU_US_rebuliding_trust_EN.pdf.

2 EDRI (2012) Position on the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Доступно через: https://edri.org/files/1012EDRi_full_position.pdf.

3 Там же

ное обсуждение вопроса гражданами, правозащитными группами, коммерческими компаниями и государственными органами.

Принцип 4: Ничем не ограниченный перехват электронных коммуникаций неприемлем. Сбор данных в интересах наблюдения и контроля (surveilance) должен быть нацеленным и ограничен рамками, пропорциональными целям такого наблюдения.

Принцип 5: Законы должны быть четкими, и должна поддерживаться их актуальность. Нельзя, чтобы страны-члены Евросоюза, устанавливая рамки современных программ контроля и наблюдении, полагались на устаревшие законы, разработанные в другую технологическую эпоху. Такие законы мало или вообще ничего не говорят гражданам о том, что на самом деле происходит.

Принцип 6: Исключения со ссылкой на интересы национальной безопасности должны использоваться экономно. Они должны быть именно исключениями, а не правилом. Необходимость защиты национальной безопасности может оправдать особые нормы. Однако не всё, что относится к внешним связям, является вопросами национальной безопасности. Иной подход подрывает легитимность законов, имеющих жизненно важное значение для нашей безопасности.

Принцип 7: Судебный надзор необходимо для того, чтобы избежать слишком сильного «раскачивания маятника» в разные стороны. Надзор со стороны исполнительной власти – дело хорошее. Парламентский контроль необходим. Судебный же надзор является ключевым фактором.

Принцип 8: Законодательство о защите персональных данных должно применяться независимо от гражданства заинтересованных лиц. Применение различных стандартов в зависимости от того, является ли лицо гражданином данной страны, не имеет никакого смысла ввиду открытой природы интернета[1].

1 Eecke, P. (2014) EUROPE: EU Commissioner Reding introduces her Eight Principles of Data Protection. Доступно через: http://www.jdsupra.com/legalnews/europe-eu-commissioner-reding-introduc-85150/.

АМЕРИКАНО-ЕВРОПЕЙСКОЕ СОГЛАШЕНИЕ О «БЕЗОПАСНОЙ ГАВАНИ»

Подход США к вопросу неприкосновенности личной жизни в отличие от европейского носит узконаправленный характер и затрагивает конкретные сферы[1]. Он сосредоточен на потребности бизнеса и рынка в свободе передачи данных: неприкосновенность личной жизни – это тема, которая должна в первую очередь заботить бизнес с точки зрения сохранения доверия потребителя к электронным услугам. Поэтому источником соответствующих мер реагирования должно быть саморегулирование отрасли[2].

Различные подходы ЕС и США противоречили друг другу. Назрела необходимость их урегулирования и поиска компромисса с целью поддержания нормальных экономических отношений. После двух лет интенсивных переговоров стороны достигли согласия в вопросе трансграничных потоков данных, подписав в 2000 г Соглашение о «безопасной гавани». Соглашение содержит ряд принципов, аналогичных положениям 108-й Конвенции Совета Европы, «Руководящим принципам» ОЭСР и Директиве Европейского союза 1995 г. Чтобы обеспечить адекватный уровень защиты согласно требованиям директивы ЕС, компании США в добровольном порядке обязались соблюдать эти принципы. Система подвергается критике за недостаточность мер, обеспечивающих защиту неприкосновенности личной жизни применительно к личным данным европейских граждан[3]

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В СНГ

К настоящему моменту существует четыре документа, разработанных в рамках СНГ:

- *Модельный закон СНГ, принятый Межпарламентской ассамблеей в 1999 г. http://www.russianlaw.net/law/civil_rights/pd/t20/;*
- *Решение Координационного Совета государств-участников СНГ по информатизации при РСС от 1 июля 2003 г. N 3/1. «Стратегия сотрудничества стран СНГ в сфере информатизации» http://www.cis.minsk.by/page.php?id=3558;*
- *Решение Совета глав правительств Содружества Независимых Государств «О внесении дополнений в Стратегию сотрудничества государств - участников СНГ в сфере информатизации и в План действий по реализации Стратегии сотрудничества государств - участников СНГ в сфере информатизации на период до 2010 года» http://www.levonevski.net/pravo/norm2013/num18/d18753.html;*
- *Соглашение о сотрудничестве в создании государственных информационных систем паспортно-визовых документов нового поколения и дальнейшем их развитии и использовании в государствах – участниках СНГ (2009) http://cis.minsk.by/reestr/ru/index.html#reestr/view/text?doc=2550;*

1 Loring T (2002) An analysis of the informational privacy protection afforded by the European Union and the United States. http://www.highbeam.com/doc/1P3-114483467.html.
2 Federal Trade Commission (1998) Privacy online: a report to Congress. http://www.ftc.gov/reports/privacy3/toc.shtm.
3 Galexia (2008) The US Safe Harbor – Fact or Fiction? http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safeharbor_fact_or_fiction-Introduc.html.

Модельный закон, как и все упомянутые выше документы, включает основные принципы документа ОЭСР 1980 г. В других документах даются определения ключевых терминов, имеющих отношение к обеспечению качества данных и защите прав субъектов персональных данных.

Таким образом, широкое распространение практики сбора данных вкупе со свободной их передачей (или в условиях отсутствия ограничений потока данных) могут подорвать существующие механизмы защиты данных. Поэтому в настоящее время актуализировалась задача пересмотра международных правовых документов, предусматривающих обеспечение защиты данных, чтобы оценить, продолжают ли изложенные в них концепции защиты данных соответствовать реалиям настоящего времени. Не уменьшающаяся, а скорее, все возрастающая актуальность вопросов защиты частной жизни в цифровой среде, является движущим фактором разработки новых документов на международном уровне. В 2013 году Генеральная Ассамблея ООН приняла специальную резолюцию, посвященную защите приватности в цифровой век[1], что было вызвано не только политическим скандалом, связанным с разглашением сотрудником спецслужб США Сноуденом сведений о перехвате электронный коммуникаций системой PRISM[2]. Ведь аналогичный скандал уже имел место пятнадцать лет назад, только система слежки тогда называлась ECHELON[3]. На этот раз разглашение затронуло очень тонкую сферу – управление Интернетом и имело далеко идущие последствия. В результате появилось заявление технического сообщества Интернета, подписанное главными его администраторами, в котором они выразили «серьезную обеспокоенность подрывом доверия пользователей интернета во всем мире в свете появившейся недавно информации о повсеместном наблюдении и надзоре» [4].

Заявление поставило под сомнение способность США гарантировать свободу Интернета в условиях функционирования системы глобальной слежки в сети. Это послужило импульсом для еще одного решения, уже со стороны Национальной администрации электросвязи США инициировать процесс глобализации администрирования адресных ресурсов с передачей «попечительской» функции от правительства США техническому сообществу в марте 2014 года[5]. Время покажет искренность этих заявлений и их реальное воплощение, однако это не снимает с повестки дня вопрос о дальнейшем развитии Интернета как универсальной, открытой и свободной для подключения сети. Ведь доверие, которое является основой дальнейшего роста подключений и развития сервисов не может быть достигнуто без надлежащих гарантий защиты приватности и безопасности.

1 Резолюция 68/167. Право на неприкосновенность личной жизни в цифровой век, ГА ООН, 18 декабря 2013. (UN Doc A/C.3/68/L.45/Rev.1) http://www.un.org/ru/documents/ods.asp?m=A/RES/68/167
2 https://ru.wikipedia.org/wiki/PRISM_(программа_разведки)
3 http://en.wikipedia.org/wiki/ECHELON
4 Заявление о будущем сотрудничества в сфере интернета, Монтевидео, Уругвай, 7 октября 2013 года, https://www.icann.org/news/announcement-2013-10-07-ru?routing_type=path
5 Передача координирующей роли NTIA в осуществлении функций IANA, https://www.icann.org/ru/stewardship

НАЦИОНАЛЬНЫЕ РЕЖИМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ

Ключевые слова: субъект персональных данных, держатель персональных данных, пользователь персональных данных, обработчик персональных данных, сборщик персональных данных, контролер файлов, пользователь данных

Как уже отмечалось выше, правовой режим защиты персональных данных зависит от исторического и культурного контекста, традиций управления, специфики процесса принятия политических решений и выработки законодательства.

Практически во все национальные законодательные акты вошли полностью или частично положения, закреплённые в Руководящих принципах ОЭСР. Однако включение этих принципов в национальные законодательные акты столкнулось с определёнными трудностями. Вот только некоторые из этих проблем:

- *как регулировать повторное использование данных;*
- *каковы основы ограничений на сбор информации;*
- *как организации должны доказать, что собираемые данные соответствуют заявленным целям сбора;*
- *как определить обстоятельства, при которых необходимо формальное согласие субъекта данных и при которых такое согласие может рассматриваться как само собой разумеющееся;*
- *как определить различия между сбором, использованием и разглашением информации, можно ли отказаться от этих различий и обозначать все эти процессы общим термином «обработка информации»*[1].

Международно-правовые обязательства государств по защите персональных данных граждан соответствующим образом корреспондируют индивидуальным правам, которые гарантируются и должны быть эффективно защищены со стороны государства. Очевидным следствием этого является обязанность правительств контролировать соблюдением этих прав и проводить необходимый комплекс мероприятий по защите персональных данных индивида: вырабатывать строгие принципиальные положения, касающиеся требований по сбору, доступу, хранению, использованию, распространению и защите персональных данных.

Правовой режим защиты персональных данных зависит от исторического и культурного контекста, традиций управления, специфики процесса принятия политических решений и выработки законодательства. Однако практически во все национальные законодательные акты вошли полностью или частично положения, закреплённые в Руководящих принципах ОЭСР.

Первые законодательные акты в отношении персональных данных принимались в связи с созданием централизованных государственных баз данных уже в 1960-х гг. Однако нормы, принимавшиеся до 1970 г. носили в основном, технический характер. Номы второй половины 1970-х годов гораздо больше внимания уделяли правам индивидов. Третье поколение норм связано с реакцией на введение концепта «информационного самоопределения личности» в немецком законодательстве. Четвертое поколение норм связано с разработкой секторальных законов, дополняющих общие законы о защите персональных данных.

1 Bennett, 2008. P.8

Основы надлежащего отношения к информационной приватности были сформулированы в Европе и США в конце 1960 - начале 1970-х гг.[1]

В 1969 году Парламент Великобритания принял «Билль о наблюдении за данными», устанавливающий контроль над использованием собранной информации о подданных.

В 1970 и 1971 годах Канада и Австралия приняли соответственно Законы "О секретности" и "О нарушении секретности", которые использовали принципы защиты информации, применявшиеся в США и Великобритании.

Первым целевым законодательным актом по защите персональных данных является немецкий Закон Земли Гессен 1970 года "О защите данных". Это один из наиболее удачных законов первого поколения, который продолжает считаться образцом в этой области. Авторы Закона, исходя из предпосылки, что информационные потоки формируют "нервный центр общественной жизни» и обладание информацией о гражданах представляет «общественную силу», справедливо полагали, что автоматизированная обработка данных без принятия мер по их защите несет угрозу личной свободе и, как следствие, создает новую угрозу гражданскому обществу. На базе Закона Земли Гессен 1970 года был разработан и принят в 1990 году федеральный Закон "О дальнейшем развитии обработки данных и защиты данных". Его главная цель предусматривала обязанность "защитить лицо от ущемления его прав вследствие ознакомления с его персональными данными". Сфера применения Закона распространялась на любые действия государственных и негосударственных организаций, связанные с получением, обработкой, хранением и распространением персональных данных, при использовании традиционных или автоматизированных средств.

Закон "О данных" Швеции был принят в 1972 году. Он предусматривал введение инспекции по вычислительной технике (государственного учреждения), на которую возлагались обязанности по контролю персональных данных, хранящихся в автоматизированных системах. Создание какой бы то ни было картотеки персональных данных предусматривает получение разрешения инспекции, предоставляющей инструкции, необходимые для устранения риска нарушения прав личности. В 1973 году Парламент Швеции принял Закон "О вычислительной технике". Закон вводил перечень преступлений нового типа – за нарушение прав личности посредством операций с вычислительной техникой, и устанавливал соответствующие санкции.

В январе 1978 года во Франции был принят Закон "Об информатике, картотеках и свободах". Французское законодательство использовало опыт регулирования процессов обработки информации персонального характера, накопленный в США, Германии, Швеции и др. странах, однако применительно только к автоматизированным средствам, традиционные формы работы с картотеками на бумажном носителе под его действие не подпадали. При этом, если порядок автоматизированной обработки информации был детально регламентирован, то регулирование сбора, хранения и распространения информации носило довольно общий характер.

Принципы добросовестного отношения к сведениям об индивидах, собираемых частными и общественными организациями, впервые были сформулированы в США.

Первоначально таких принципов было 5:

1 Bennett, C. (1992) Regulating Privacy: Data Protection and Public Policy in Europe and the United States. Ithaca, NY: Cornell University Press

1. не должно существовать никаких секретных баз персональных данных (принцип открытости);
2. индивиду должна предоставляться возможность узнать, какая информация о нем собрана и как она используется (принцип доступа);
3. необходимо предпринять меры для того, чтобы информация, собранная для одних целей, не использовалась для других без согласия индивида;
4. необходимо обеспечить индивидам возможность исправлять или дополнять информацию о себе (принцип участия);
5. любая организация, создающая, хранящая, использующая или распространяющая данные, по которым можно идентифицировать индивида, должна обеспечить надежность данных и должна принять необходимые меры для предотвращения ненадлежащего использования этих данных (принцип качественного управления информацией).[1]

В 1977 г. был опубликован отчет Комиссии по изучению защиты приватности, в тринадцатой главе которого было изложено уже семь принципов. В их число входили уточнённые принципы открытости, доступа, участия и качественного управления информацией, а также четыре новых требования:

- *принцип ограничения сбора как типов данных, которые организация может собирать об индивиде, так и способов такого сбора;*
- *принцип ограничения использования – ограничение использования данных об индивидах в рамках организации, которая имеет эти данные;*
- *принцип ограничения разглашения информации об индивиде;*
- *принцип отчетности организации, в соответствии с которым, они должны информировать общественность о политике, практике и системах сбора информации.*

Несмотря на все национальные особенности, в различных правовых системах использовались только два принципиально отличавшихся подхода.

Несмотря на все национальные особенности, в различных правовых системах использовались только два принципиально отличавшихся подхода.

- *Генеральный – заключался в стремлении к созданию единого и всеобъемлющего закона о защите сферы частной жизни и был связан с попытками теоретического обоснования некоего «всеобщего и абсолютного права на невмешательство в частную жизнь». Некоторые страны включили право на защиту персональных данных в Конституцию (Швеция, Бельгия, Греция, Нидерланды).*
- *Секторный (или отраслевой) – состоял в создании специализированных законов либо для каждого типа посягательств на сферу частной жизни, либо для каждой отрасли или сектора человеческой деятельности, являющейся потенциальным источником угроз для права человека на невмешательство в его частную жизнь (например, для почты и средств связи, для бюро кредитной информации, для средств массовой информации и рекламной сферы, для частных детективов, для компьютерных банков данных. Отраслевые законы представляют собой дополнительные законоположения, конкретизирующие положения базового национального закона о защите данных и обеспечивающие защиту персональных данных в отраслях человеческой деятельности, связанных с обработкой, передачей или использованием таких данных и несущих потенциальные угрозы посяга-*

1 Gellman, R. (2014) Fair Information Practices: A Basic History < http://www.bobgellman.com/rg-docs/rg-FIPShistory.pdf>

тельства на сферу частной жизни граждан. «Секторный» («отраслевой») подход предполагающий, что новые «отраслевые» законы принимаются по мере накопления прецедентной базы, указывающей на новый источник угроз для сферы частной жизни, приводил к бессистемности, дублированию и противоречивости законоположений.

Уже в конце 1990-х гг. эксперты отмечали, что в чистом виде и тот, и другой подходы оказались непродуктивными. В подавляющем большинстве стран современные национальные системы правового регулирования обработки и использования персональных данных применяют так называемый смешанный принцип, объединяющий определенные аспекты «генерального» и «отраслевого» подходов.

Национальное законодательство в сфере защиты данных, как правило, состоит из базового или системообразующего закона и комплекса отраслевых законов, обеспечивающих защиту персональных данных в различных контекстах. Регулирующими компонентами современных систем защиты персональных данных являются также национальный уполномоченный орган (или система органов) по защите данных и корпоративные средства защиты (саморегулирование в форме кодексов поведения/практики).

Национальное законодательство в сфере защиты данных, как правило, состоит из:

- *базового или системообразующего закона;*
- *комплекса отраслевых законов, обеспечивающих защиту персональных данных в различных контекстах.*

Регулирующими компонентами современных систем защиты персональных данных являются также национальный уполномоченный орган (или система органов) по защите данных и корпоративные средства защиты (саморегулирование в форме кодексов поведения/практики).

Национальный орган (или органы) по защите данных, как правило, наделяются регистрационно-разрешительными, контрольно-надзорными, арбитражными, экспертными и методологическими функциями.

Хотя процедурные нормы излагаются по-разному, в соответствии с правовой системой каждой страны, существует широкое согласие в отношении целей, которые должны быть обеспечены этими нормами.

Хотя процедурные нормы излагаются по-разному, в соответствии с правовой системой каждой страны, существует широкое согласие в отношении целей, которые должны быть обеспечены этими нормами. Национальные законодательства, включают, как минимум, следующие принципы, зафиксированные в международных документах:

- *открытость – общество должно быть проинформировано о наличии баз персональных данных, которые находятся в распоряжении правительственных органов, организаций и учреждений;*
- *возможность доступа субъекта данных к данным о себе и возможность корректировать неточные или устаревшие данные;*
- *сбор персональных данных и объем этих данных должен быть ограничен в соответствии с целями сбора;*
- *ограничение использования – персональные данные должны использоваться только в целях, для которых они собирались;*

- *ограничения раскрытия – персональные данные могут быть раскрыты только в законных целях и с согласия субъекта данных[1];*
- *безопасность – данные должны быть защищены от потери, несанкционированных доступа, уничтожения, использования или модификации[2].*

В США и некоторых странах Азии защита персональных данных обеспечивается, главным образом, за счет саморегулирования, осуществляемого частными и государственными институтами. Правовой режим США определяется тем, что эффективность бизнеса и государственного управления рассматриваются как приоритетные цели, а защита персональных данных – как инструментальная ценность.

В США нет общего закон о защите персональных данных. Права граждан в этой сфере обеспечиваются рядом отраслевых актов:

- *Закон США о защите частных прав ребёнка в интернете (Children's Online Privacy Protection Act/COPPA, 1998),*
- *Закон США об отчетности и безопасности медицинского страхования (Health Insurance Portability and Accountability Act/HIPAA, 1996) и др.*

Модель защиты персональных данных в странах Европейского Союза строится на основании общих правил защиты персональных данных, изложенных в Директиве ЕС 1995 г.

В некоторых национальных правовых системах защиты данных системообразующее законодательное ядро состоит не из одного, а из двух взаимодополняющих законов – о защите персональних данных (Data Protecton Act) и о свободе информации (Information Freedom Act).

В некоторых национальных правовых системах защиты данных системообразующее законодательное ядро состоит не из одного, а из двух взаимодополняющих законов - о защите персональних даннях (Data Protecton Act) и о свободе информации (Information Freedom Act), которые нередко даже разрабатываются и принимаются одновременно. В других системах принцип свободы доступа к информации непосредственно закладывается в положениях закона о защите персональных данных.

Структура законов, в большинстве случаев, включает принципы качества персональных данных; права субъекта данных в связи с обработкой и использованием данных о нем; установленные законом правила доступа к чужим персональным данным, их раскрытия и передачи; исключения из правил в интересах государственной и общественной безопасности, в связи с расследованием преступлений и т. п. (например, сбор данных без согласия индивидов); установленные законом меры правового регулирования сбора, хранения, обработки, передачи и использования персональных данных; учреждение национального органа власти (или системы органов власти) по защите персональных данных, регистрация (или лицензирование) обработки персональных данных; создание и ведение национальных регистров держателей и пользователей персональных данных, лицензирование передачи персональных данных за пределы национальной территории; требования к организационно-техническим мерам по обеспечению безопасности данных при их сборе, обработке,

1 (Bennett, 1988a; 1992: 101-111)
2 Hert, P. (2013) Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency? < http://moritzlaw.osu.edu/students/groups/is/files/2013/08/7-Hert-Papakonstantinou.pdf>

использовании, передаче и хранении; статьи, устанавливающие наказания за нарушения принципов защиты данных и иных положений закона о защите данных[1].

Структура законов, в большинстве случаев, включает:

1. *принципы качества персональных данных;*
2. *права субъекта данных в связи с обработкой и использованием данных о нем;*
3. *установленные законом правила доступа к чужим персональным данным, их раскрытия и передачи;*
4. *исключения из правил в интересах государственной и общественной безопасности, в связи с расследованием преступлений и т. п. (например, сбор данных без согласия индивидов);*
5. *установленные законом меры правового регулирования сбора, хранения, обработки, передачи и использования персональных данных;*
6. *полномочия национального органа власти (или системы органов власти) по защите персональных данных,*
7. *требования к организационно-техническим мерам по обеспечению безопасности данных при их сборе, обработке, использовании, передаче и хранении;*
8. *статьи, устанавливающие наказания за нарушения принципов защиты данных и иных положений закона о защите данных*

Отраслевые законы редко разрабатываются специально для конкретного вида угроз качеству данных или правам субъектов данных. Дополнительные положения о защите персональных данных включаются в уже существующие или разрабатываемые законы, регламентирующие все аспекты деятельности в той или иной отрасли по мере накопления прецедентной базы посягательств на права субъектов персональных данных в конкретной отрасли. Основное достоинство иерархической системы «базовый закон – отраслевые законы» состоит в том, что при появлении новых видов неправомерных посягательств на персональные данные нет необходимости пересматривать всю систему юридических гарантий.

Национальные законы включают, в целом, сходный субъектный состав информационных правовых отношений, возникающих в процессе сбора, хранения, обработки, использования и передачи персональных данных

Национальные законы включают, в целом, сходный субъектный состав информационных правовых отношений, возникающих в процессе сбора, хранения, обработки, использования и передачи персональных данных:

а) лица, физические и юридические (как правило, физические), к которым относятся собираемые, хранимые, обрабатываемые, используемые и передаваемые данные. В информационном праве подавляющего большинства стран для обозначения этих лиц применяется термин «субъект данных» (data subject); в некоторых законах используется термин термин «заинтересованное лицо», который имеет более широкое значение в сфере обработки и использования персональных данных:

1 Иванский, В.П. (1999) Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования. Москва, РУДН. - 276с. http://www.pravo.vuzlib.su/book_z137_page_1.html

- *Субъект персональных данных - физическое лицо, идентифицируемое на основании этих данных (или с помощью этих данных и иной информации, находящейся в распоряжении пользователя данных);*

  б) лица, юридические и физические, осуществляющие действия по обработке и/или использованию или передаче персональных данных. В число лиц, осуществляющих действия по обработке и/или использованию или передаче персональных данных, как правило, включаются:

- *Держатель персональных данных (контролер или распорядитель файлов) - физическое или юридическое лицо, обладающее правом принимать любые (в рамках закона) решения в отношении обработки, использования и передачи компьютеризованного или основанного на иной технологии собрания персональных данных в качестве: (1) зарегистрированного и/или лицензированного собственника или владельца соответствующих информационных ресурсов; (2) лица, специально уполномоченные компетентными государственными органами.*
- *Пользователь персональных данных - физическое или юридическое лицо, по установленной законом процедуре, использующее собранные и обработанные персональные данные, для которых оно не является «держателем данных» («контролером файлов»).*
- *Обработчик персональных данных - физическое или юридическое лицо, располагающее компьютерными или иными мощностями, лицензированными для требуемой обработки персональных данных, и осуществляющее автоматизированную или ручную обработку данных, для которых оно не является «держателем данных» («контролером файлов») и которые он получает от коммерческого заказчика или иного лица, обладающего правами «держателя» этих данных.*
- *Сборщик персональных данных - физическое или юридическое лицо, осуществляющее первичный сбор персональных данных в соответствии с собственными законными полномочиями или по поручению лица, обладающего такими полномочиями[1].*

Национальные законы дают сходные нормативные определения понятия «субъект данных», хотя встречаются некоторые отличия, не связанные с действующей системой права или государственным устройством страны, которые зависят от национальных традиций и особенностей национального языка.

> Финский закон 1988 г. о файлах персональных данных определяет "субъект данных" таким образом: "...§ 4. Термин "субъект данных" означает любое лицо, к которому относятся персональные данные".
>
> Британский законодательный акт 1984 г. о защите данных определяет это понятие так: "...4) Под "субъектом данных" понимается индивидуум, являющийся субъектом персональных данных".
>
> Австрийский закон 1978 г. о защите данных распространяет понятие "персональные данные" и на сведения об организациях (только частного права), т.е. признает право на невмешательство в "корпоративную частную сферу":"...§ 2. Субъект данных: любое физическое или юридическое лицо, или ассоциация, отличные от контролера данных (§ 3), чьи данные используются (§ 12); юридические лица публичного права и их органы не должны рассматриваться как субъекты данных, поскольку они исполняют официальные функции"[2].

1 Иванский, В.П. (1999) Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования. Москва, РУДН. - 276с. http://www.pravo.vuzlib.su/book_z137_page_1.html
2 Там же

Японский закон 1989 г. об обрабатываемых компьютерами персональных данных, хранимых административными органами, вводит понятие "субъект обработанных данных" (ст. 2), сопоставляя его не с любыми персональными данными, а с данными, специально организованными в файл персональных данных для определенной цели:

1. Термин "файл персональных данных" означает любую группу персональных данных, систематически собранных и организованных для достижения цели (завершения выполнения) определенных функций, которые должны быть записаны на магнитной ленте, магнитном диске или любом другом подобном носителе, способном сохранять определенные данные надежно зафиксированными для целей компьютерной обработки.

2. Термин "обработанные данные" означает персональные данные, записанные в некоем файле персональных данных.

3.Термин "субъект обработанных данных" означает любого индивидуума, данные о личности которого могут быть воспроизведены и выделены в ходе компьютерной обработки без ссылок на принадлежащие любому другому индивидууму имя, дату рождения, иные описания или номера, символы, иные признаки, присвоенные другому индивидууму среди индивидуумов, идентифицируемых этими обработанными данными"[1].

В 1981 г. Конвенция 108 Совета Европы с целью гармонизации терминологии в области защиты персональных данных ввела новый термин «контролер файлов» (file controller), определяемый следующим образом: "ст. 2...d) под термином "контролер файлов" понимается физическое или юридическое лицо, орган публичной власти, ведомство или любая другая организация, которые в соответствии с национальным правом, наделены полномочиями решать для какой цели создается файл данных, какие категории персональных данных будут в нем накапливаться и какие операции с ними будут осуществляться.

В определении Бельгийского закона 1992 г. о защите персональной приватности при обработке персональных данных сказывается гармонизирующее влияние Конвенции 108: «Термин «контролер файла» означает любое физическое или юридическое лицо или ассоциацию де-факто, наделенные правом принимать решения относительно целей обработки и типа данных, которые должны быть обработаны. В случае, когда цели обработки и тип данных, которые должны быть обработаны, установлены законом, контролер файла должен быть физическим или юридическим лицом, назначенным этим законом для контроля (управления) данного файла...».

Аналогичным образом подходит к определению этого понятия и Финский закон 1988 г. о файлах персональных данных:"...3. Термин "контролер файла" означает любое юридическое лицо, ассоциацию или фонд, которые учреждены для использования файла персональных данных и которое имеют право распоряжения над использованием этого файла персональных данных.

Национальные законы по защите персональных данных не содержат положений, устанавливающих права собственности держателей данных (контролеров файлов) по отношению к компьютеризованным или ручным собраниям персональных данных. Установление прав собственности на данные всех видов (а не только персональные) и их собрания производится в других разделах информационного права.

1 См.: Art. 2(6) of The Act for Protection of Computer-Processed Personal Data Held by Administrative Organs (1989, Japan).Иванский, В.П. (1999) Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования. Москва, РУДН. - 276с. http://www.pravo.vuzlib.su/book_z137_page_1.html

Следует отметить, что в настоящее время понятие «контролер данных» подвергается серьезному пересмотру в контексте современного сетевого общества. Рост сложности бизнес моделей и отношений (субподряды, аутсорсинг, поведенческая реклама и пр.), а также развитие технологий (RFID, Web 2.0) требуют введения новых уровней и степени ответственных лиц. Часто учреждение или лицо, являющееся контролером данных в одних ситуациях, может быть со-контролером, обработчиком или суб-обработчиком в других.

Наиболее распространенной категорией субъектов информационных отношений, чей статус и терминологическое обозначение определяются видом осуществляемых ими действий по отношению к персональным данным, является «пользователь данных» (data user). В большинстве национальных правовых систем *«пользователь данных»* определяется как физическое или юридическое лицо, использующее собранные и обработанные данные, для которых оно не является «держателем данных» («контролером файлов») или «обработчиком данных».

> Несколько реже в национальном законодательстве используется категория *«обработчик данных»* (data processor) или просто «обработчик» (processor), определяемый обычно как физическое или юридическое лицо, осуществляющее автоматизированную или ручную обработку данных, для которых оно не является «держателем данных» («контролером файлов») или «сборщиком данных». На практике, это лица, располагающие компьютерными или иными мощностями для требуемой обработки персональных данных, которые они получают от коммерческого заказчика или вышестоящей организации как своего рода «сырье», в отношении которого они не могут принимать никаких самостоятельных решений.
>
> Разработанный одним из первых Австрийский закон 1978 г. о защите данных использует термин "обслуживающий обработчик" (service processor):"ст. 3(4). Обслуживающий обработчик: любое лицо или орган юридического лица публичного права, использующие данные на основе такого мандата от контролера данных, который специально ориентирован на автоматизированную обработку данных"[1].
>
> Более традиционно определение из Бельгийского закона 1992 г. о защите персональной приватности при обработке персональных данных: "...(7) Термин "обработчик" означает любое физическое или юридическое лицо, или ассоциацию де-факто, на которые возложены обязанность и ответственность за организацию и выполнение обработки"[2].

И совсем редко используется категория «сборщик данных» (data collector), под которым подразумевается (судя по контексту использования этого термина) либо лицо, осуществляющее первичный сбор персональных данных, либо лицо, накапливающее персональные данные в своей информационной системе. Этот термин эпизодически применяется в зарубежных законах о защите персональных данных, но не имеет определения ни в одном из них.

Помимо перечисленных выше категорий информационного права, встречается еще такая редкая категория, как «третья сторона» или «третье лицо» в сфере обработки и использования персональных данных.

> ст. 3(9). Германского федерального закона 1977 г. о защите данных: "Третьим лицом является любое лицо или учреждение вне инстанции, накапливающей данные. Третьими лицами не могут быть сам индивидуум, о котором собирают-

1 Sec. 3 of Austrian Data Protection Act (1978)

2 Art. 1(7) of Law Concerning the Protection of Personal Privacy in Relation to the Processing of Personal Data (1992, Belgium

ся данные, а также лица и учреждения, которые по поручению обрабатывают и используют данные о личности в сфере, подпадающей под действие данного закона".

Неправомерные действия по сбору, хранению, обработке, использованию или передаче персональных данных составляют посягательство на право субъекта этих данных на невмешательство в его сферу частной жизни.

Неправомерные действия по сбору, хранению, обработке, использованию или передаче персональных данных составляют посягательство на право субъекта этих данных на невмешательство в его сферу частной жизни.

Таким образом, национальное законодательство в сфере защиты данных, как правило, состоит из базового или системообразующего закона и комплекса отраслевых законов, обеспечивающих защиту персональных данных в различных контекстах. Регулирующими компонентами современных систем защиты персональных данных являются также национальный уполномоченный орган (или система органов) по защите данных и корпоративные средства защиты (саморегулирование в форме кодексов поведения/практики).

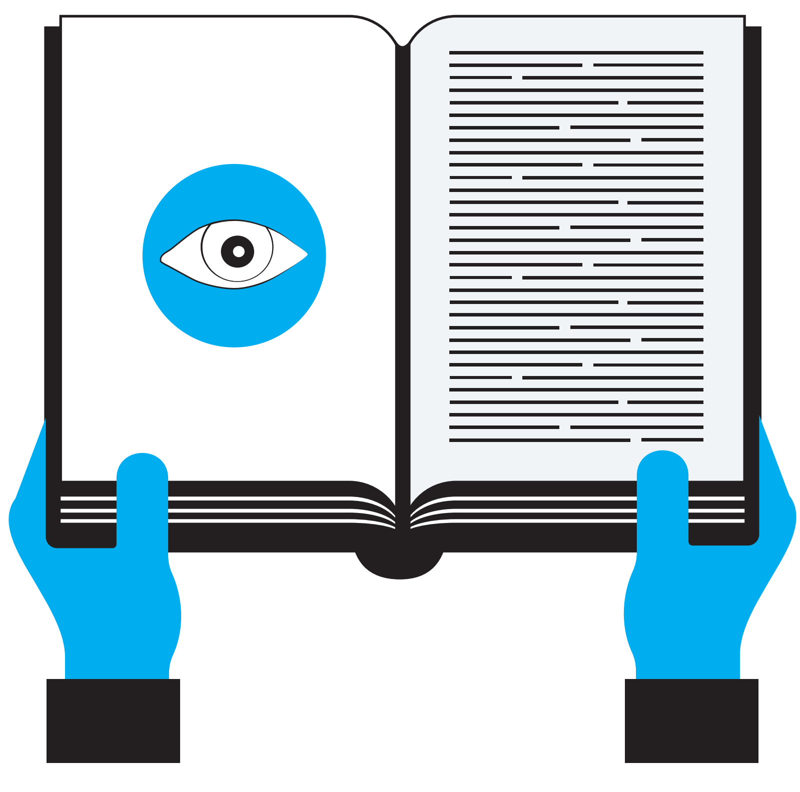
Хотя процедурные нормы излагаются по-разному, в соответствии с правовой системой каждой страны, существует широкое согласие в отношении целей, которые должны быть обеспечены этими нормами:

- *открытость и прозрачность деятельности государственных органов;*
- *возможность доступа субъекта данных к данным о себе и возможность корректировать неточные или устаревшие данные;*
- *минимизация сбора персональных данных и четкое определение цели их сбора;*
- *ограничение использования – персональные данные должны использоваться только в целях, для которых они собирались;*
- *ограничения раскрытия – персональные данные могут быть раскрыты только в законных целях и с согласия субъекта данных;*
- *обеспечение безопасности сбора, хранения и обработки данных.*

Национальные законы включают, в целом, сходный «реестр» субъектов информационных правовых отношений, возникающих в процессе сбора, хранения, обработки, использования и передачи персональных данных.

Раздел 4.

ИТОГОВЫЙ ПРАКТИКУМ



ВОПРОСЫ ДЛЯ СРАВНИТЕЛЬНОГО АНАЛИЗА ЗАКОНОДАТЕЛЬСТВА

НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ

1. Национальные законодательные акты, регулирующие права на уважение частной жизни и свободу выражения мнения
2. Область действия этих законодательных актов, субъекты и объекты регулирования
3. Содержание права на неприкосновенность частной жизни
4. Меры по недопущению нарушения права на уважение частной жизни, формы ответственности за нарушения

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Общие законодательные нормы

1. Законодательные акты, регулирующие сбор и использование персональных данных
2. Сфера регулирования, объекты и субъекты регулирования
3. Определение термина «персональные данные»
4. Предусмотрено ли создание Уполномоченного (органа/комиссии/должностного лица) по защите персональных данных?
5. Типы данных, защищаемые законодательством
6. Формы деятельности (действия в отношении персональных данных), которые регулируются законодательством
7. Требуется ли уведомление или регистрация перед обработкой персональных данных?
8. Основные исключения

Основные правила и принципы

1. Каковы основные обязанности контролеров данных по обеспечению надлежащей обработки данных?
2. Требуется согласие субъекта данных перед началом обработки?

3. Если согласие не дано, на каких других основаниях могут обрабатываться данные?
4. Существуют ли специальные правила обработки для специфических типов данных (например, уязвимых данных)?

ПРАВА ИНДИВИДОВ

1. Какая информация должна быть предоставлена субъектам данных при сборе данных?
2. Какими еще правами обладают субъекты данных?
3. Имеют ли субъекты данных право требовать удаления данных?

ТРЕБОВАНИЯ БЕЗОПАСНОСТИ

1. Каковы требования безопасности, установленные в отношении персональных данных?
2. Предусмотрена ли необходимость уведомления о нарушениях безопасности и утечках субъектов данных или национальных регуляторов?

ОБРАБОТКА ТРЕТЬИМИ СТОРОНАМИ

1. Каковы дополнительные требования при обработке данных третьими сторонами по поручению контролера данных?
2. Электронная коммуникация
3. При каких условиях контролеры данных могут хранить файлы cookies или эквивалентную информацию о терминалах субъектов данных?

МЕЖДУНАРОДНЫЙ ОБМЕН ДАННЫМИ

1. Какие правила регулируют передачу данных за пределы национальной юрисдикции?
2. Обсуждаются ли/приняты ли соглашения о передаче данных других государств?
3. Существуют ли стандартные формы или одобренные властями прецеденты передачи данных за границу?
4. В достаточной ли степени соглашение о передаче данных защищает права субъектов персональных данных или необходимы дополнительные нормы?

5. Должен ли национальный регулятор одобрить передачу данных за границу?

ПРАВОПРИМЕНЕНИЕ И САНКЦИИ

1. Каковы права национального регулятора?
2. Какие санкции предусмотрены за нарушение законодательства о защите персональных данных

ИЗБРАННАЯ БИБЛИОГРАФИЯ

Учебники

1. Баранов А., Брыжко В. Базанов, Ю. (2010) Права человека и защита персональных данных. Доступно через: http://www.lawtrend.org/information-access/prosto-o-vaznom/prava-cheloveka-i-zashhita-personalnyh-dannyh.
2. Василевич, Г. (2013) Информационное право.
3. Великомыслов Ю., Равлик А. (2005) Пособие по защите Ваших прав в сети Интернет. Доступно через: http://allpravo.ru/library/doc2044p/instrum4935/
4. Иванский, В.П. (1999) Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования. Доступно через: http://www.pravo.vuzlib.su/book_z137_page_1.html.
5. Кочева О., Маковецкая С.., Малых И., Теплых Л. (2007) Лучше понимаем про право на неприкосновенность частной жизни": справочник для методичных любопытствующих. Доступно через: http://www.pgpalata.ru/reshr/privacy/10.shtml.
6. Сморгунов, Л. (2006) Государственная политика и управление. Доступно через: http://gpb22.narod.ru/smorgunov_1/chapter14.html.
7. Задорожний А., Пазюк А.(2013) Международное информационное право.

Справочники

1. Гомен, Д. (2000) Путеводитель по европейской Конвенции прав человека. Совет Европы.
2. Европейская Комиссия. Генеральный Директорат по Коммуникациям (2013) Как работает Европейский Союз. Ваш гид по институтам ЕС. Доступно через: http://eeas.europa.eu/delegations/russia/documents/publications/how_eu_works_2013_ru.pdf.
3. Килкелли, У., Чефранова, Е. (2001) Европейская конвенция о защите прав человека и основных свобод. Ст. 8 Право на уважение частной и семейной жизни, жилища и корреспонденции. Российская Академия правосудия. Доступно через: http://sutyajnik.ru/rus/echr/school/books/art8.pdf.
4. Килкелли, У. (2003) Право на уважение частной и семейной жизни. Гид по внедрению. Ст.8 европейской Конвенции по правам человека. Доступно через: http://edu.helsinki.org.ua/library/privatlife/povaga-do-privatnogo-ta-s-meinogo-zhittya-na-zasadakh-st-8-vropeisko-konvents-pra.
5. Кочева, О., Маковецкая С., Малых И., Теплых Л.. (2004-2007) Лучше понимаем про право на неприкосновенность частной жизни: справочник для методичных любопытствующих. Доступно через: http://www.pgpalata.ru/reshr/privacy/10.shtml.

Монографии и статьи

1. Авдеев, М.Ю. (2013) Законодательство Российской Федерации о неприкосновенности частной жизни: к вопросу о заимствовании зарубежного опыта. Доступно через: http://cyberleninka.ru/article/n/zakonodatelstvo-rossiyskoy-federatsii-o-neprikosnovennosti-chastnoy-zhizni-k-voprosu-o-zaimstvovanii-zarubezhnogo-opyta.

2. Алексеев С.С. Механизм правового регулирования в социалистическом государстве. М., 1966.

3. Андерсон, Дж. Публичная политика: введение. Доступно через: http://www.docme.ru/doc/122742/2-stat._ya-anderson-public-policy .

4. Ариков, Г. (2014) Аспекты неприкосновенности частной жизни в уголовном законодательстве Республики Молдова. Доступно через: http://www.cnaa.md/files/theses/2014/26884/gheorghii_aricov_abstract_ru.pdf.

5. Барабанов , О. (2009). Определение теоретических подходов. Проблемы глобального управления: выбор аналитической парадигмы http://www.cnaa.md/files/theses/2014/26884/gheorghii_aricov_abstract_ru.pdf. http://www.alleuropa.ru/index.php?option=com_content&task=view&id=1248

6. Бачило, И., Сергиенко Л., Кристальный Б., Арешев А..(2006) Персональные данные в структуре информационных ресурсов. Основы правового регулирования. Доступно через: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=CJI;n=13826.

7. Беляева, Н.(2001) Право на неприкосновенность частной жизни и доступ к персональным данным. Доступно через: http://www.law.edu.ru/article/article.asp?articleID=173609.

8. Беляева, Г. (2013) Правовой режим: общетеоретическое исследование. Доступно через: http://law.edu.ru/book/book.asp?bookID=1534028.

9. Березовский, К. (2012) Пределы государственной защиты персональных данных граждан в сети Интернет: международно-правовой аспект. Доступно через: http://zakon.ru/Blogs/OneBlog/2126.

10. Березовский, К. Международно-правовые обязательства Республики Беларусь в области защиты персональных данных. Доступно через: http://elib.bsu.by/handle/123456789/23916.

11. Березовский, К. (2013) Актуальные проблемы в области защиты персональных данных. Доступно через:http://elib.bsu.by/bitstream/123456789/88775/1/beresovskiy_2013_BMW.pdf.

12. Березовский К. (2011) К вопросу о международно-правовой ответственности государств в сфере защиты персональных данных // Евразийский юридический журнал. № 6. С. 57-61.

13. Березовский, К. (2012). Роль судебных прецедентов в формировании международно-правовых норм в области защиты персональных данных.

14. Ваимерш, Э. (2013) Европейские кодексы корпоративного управления и их эффективность. Доступно через: http://www.oecd.org/daf/ca/2013OECDRussiaCorporateGovernanceRoundtableEuropeanCodesRus.pdf.

15. Вайхерт, Г. (2011) Защита персональных данных в рамках серии дискуссий «Настоящее будущего». Доступно через: https://www.datenschutzzentrum.de/vortraege/20110224-weichert-datenschutz-moskau-ru.pdf.

16. Василевич, Г. (2009) Неприкосновенность частной жизни. Доступно через: http://elib.bsu.by/handle/123456789/89231.

17. Василевич, Г.(2009) Правовая защита индивидуального самоопределения. Доступно через: http://elib.bsu.by/handle/123456789/11769.

18. Важорова, М. (2011) История возникновения и становления института персональных данных. Доступно через: http://www.moluch.ru/conf/law/archive/37/365/.

19. Вельдер И. (2006) Система правовой защиты персональных данных в Европейском союзе. Доступно через: http://lawtheses.com/sistema-pravovoy-zaschity-personalnyh-dannyh-v-evropeyskom-soyuze.

20. Володина, А. (2006) Применение судами статьи 10 Европейской Конвенции и принципов, выработанных Европейским судом по правам человека при рассмотрении дел о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц. Доступно через:http://www.iteam.ru/publications/legal/section_107/article_4259/.

21. Гарфинкель, С. (2003) Все под контролем: Кто и как следит за тобой. Доступно через: http://www.uhlib.ru/kompyutery_i_internet/vse_pod_kontrolem_kto_i_kak_sledit_za_toboi/index.php.

22. Гачке, Л. (2009) Некоторые аспекты защиты прав потребителей при потребительском кредитовании. Доступно через: http://www.myshared.ru/slide/139127/.

23. Григорьев, И. (2013) Частная жизнь, ее неприкосновенность и право: соотношение понятий. Доступно через: http://tinyurl.com/lrnxqar.

24. Егошина, Г. (2014) Модернизация конституционно-правового регулирования защиты персональных данных в Европе: усиление региональной интеграции. Доступно через http://teoria-practica.ru/rus/files/arhiv_zhurnala/2014/3/yurisprudentsiya/egoshina.pdf.

25. Еллинек, Г.(2004) Общее учение о государстве. - СПб.: Юрид. центр Пресс.

26. Замошкин, Ю. (1991) Частная жизнь, частный интерес, частная собственность// Вопросы философии. 1991. M91. С. 4-5.

27. Иванский, В. (1999) Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования. Доступно через: http://www.pravo.vuzlib.su/book_z137_page_1.html.

28. Измайлова, Н. (2009) Неприкосновенность частной жизни в гражданском праве: На примере права Великобритании, США и России. Доступно через: М http://law.edu.ru/book/book.asp?bookID=1325460.

29. Кант, И. Основы метафизики нравственности // Кант И. Соч.: В 4 т. Т. 4. Ч. I. С. 290.

30. Кастиллио, М. Политика космополитизма: от универсализма к плюрализму. Доступно через: http://psibook.com/philosophy/politika-kosmopolitizma-ot-universalizma-k-plyuralizmu.html

31. Кавукиан, Э. (2011) Privacy by Design 7 основополагающих принципов. Доступно через: http://privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-russian.pdf.

32. Каламкарян, Р. (1991) Принцип добросовестности в современном международном праве. Доступно через: http://law.edu.ru/book/book.asp?bookID=53095.

33. Козик, А. (2008) Трансграничность сети Интернет и связанные с ней проблемы международно-правового регулирования Интернет // Проблемы управления. № 2.

34. Кочева, О. (2007) Уважение частной жизни в России: диагноз и прогноз. Доступно через: http://www.pgpalata.ru/reshr/privacy/art10.shtml#n3.

35. Красотенко, О.(2011) Понятие «частная жизнь» в решениях Европейского Суда по правам человека. Доступно через: http://elib.bsu.by/handle/123456789/29040.

36. Кудряков, А., Бурков А. Защита конституционных прав на неприкосновенность частной жизни, личную тайну свидетелей по делам об административных правонарушениях. Доступно через: http://www.ehu.lt/files/Journal-2013-3.pdf.

37. Кузахчетова, С. (2008) Принцип неприкосновенности частной жизни теоретико-правовой аспект. Доступно через: http://lawtheses.com/printsip-neprikosnovennosti-chastnoy-zhizni-teoretiko-pravovoy-aspekt.

38. Кузахметова, С. Неприкосновенность частной жизни -фундаментальный принцип прав человека (исторический и теоретический аспекты). Доступно через: http://www.rusnauka.com/ONG_2006/Pravo/17749.rtf.htm.

39. Кужукеева, Г. (2011) Право на частную жизнь и право на свободу выражения: проблемы соотношения. Доступно через: http://medialaw.asia/node/4318

40. Лепешкина Н. (2005). Неприкосновенность частной жизни, что это? // Адвокатская практика. № 2.

41. Майер-Шенбергер, В. Кукьер, К. (2014) Большие данные. Революция, которая изменит то, как мы живем, работаем и мыслим.

42. Мид, М. (2004) Мужское и женское. Исследования полового вопроса в изменяющемся мире.

43. Мельников, М. (2012) О семантике понятия «приватное» // XIII международная научная конференция преподавателей, аспирантов и студентов НСИ. С.181-189.

44. Малеина, М. (2001) Личные неимущественные права граждан: понятие, осуществление, защита.

45. Митцукова, Г. (2005) Право на неприкосновенность частной жизни как конституционное право человека и гражданина.

46. Назаренко, А. (2008) Контрольно-надзорный орган в системе защиты персональных данных в странах Европы. Доступно через: http://elib.bsu.by/handle/123456789/1131.

47. Новикова, А. (2010) Об уголовно-правовой защите неприкосновенности частной жизни в контексте концепции privatheit. Доступно через: http://elib.bsu.by/handle/123456789/34469.

48. Овсейко, С. (2013) Защита персональных данных: опыт правового регулирования Ч. 1. Доступно через: http://statut.by/lichnyj-jurist/14-i-have-a-right/184-18-09-2011; Ч. 2. Доступно через: http://statut.by/lichnyj-jurist/14-i-have-a-right/186-10-10-2011.

49. О'Рейли, Т. (2005) Что такое Веб 2.0. Доступно через: http://old.computerra.ru/.

50. Паризер, Э. (2012) за стеной фильтров. Что интернет скрывает от нас. Москва, Альпина.

51. Петросян, М. (1997) Право на неприкосновенность частной жизни. Доступно через: http://library.khpg.org/files/docs/Prava_Gragdan.pdf.

52. Петрыкина, Н. (2007) Правовое регулирование оборота персональных данных в России и странах ЕС (сравнительно-правовое исследование). Доступно через: http://lawtheses.com/pravovoe-regulirovanie-oborota-personalnyh-dannyh-v-rossii-i-stranahes#ixzz3ADJT6e1E.

53. Петрухин, И. (1969) Личная жизнь: пределы вмешательства. Доступно через: http://www.lawlibrary.ru/izdanie13445.html.

54. Поливанова, Д. (2009) Современное развитие права на неприкосновенность частной жизни. // Право и жизнь. № 131 (5).

55. Поливанова, Д. (2009) Понятие «частная жизнь» в свете общепризнанного права на неприкосновенность частной жизни. // Вестник Международного юридического института. № 4 (32).

56. Поливанова, Д. (2010) Международно-правовые проблемы права человека на неприкосновенность частной жизни. Доступно через: http://www.dissercat.com/content/mezhdunarodno-pravovye-problemy-prava-cheloveka-na-neprikosnovennost-chastnoi-zhizni#ixzz3ARhumfNx.

57. Прохвачева, О. (2000) Лингвокультурный концепт «приватность»: На материале американского варианта английского языка. Доступно через: http://www.dissercat.com/content/lingvokulturnyi-kontsept-privatnost-na-materiale-amerikanskogo-varianta-angliiskogo-yazyka#ixzz3AMsvTYM.

58. Романовский, Г. (1997) Конституционное регулирование права на неприкосновенность частной жизни.

59. Романовский, Г. (2001) Право на неприкосновенность частной жизни. Доступно через: http://library.nulau.edu.ua/POLN_TEXT/KNIGI_2009_2/ROMANOVSKIY_2001.pdf.

60. Романюк, И. (2013) Право личности как персональные данные. Доступно через: http://www.legeasiviata.in.ua/archive/2013/12-2/49.pdf.

61. Сехович, О. (2013) Свобода медиа и неприкосновенность частной жизни: конфликт интересов в демократическом обществе. Доступно через: http://www.ehu.lt/files/Journal-2013-3.pdf.

62. Скоробогатов, В. (2013) Саморегулирование как свойство правовой системы. Доступно через: http://www.hse.ru/data/2013/06/05/1296350015/dis%20skorob.pdf.

63. Соколова, М. (2014) Право быть забытым: Испания против Google. Доступно через: http://www.lawtrend.org/information-access/blog-information-access/pravo-byt-zabytym-evropejskij-sud-demonstriruet-nekompetentnost.

64. Соколова, М. (2011) Перспективы многостороннего диалога по вопросам управления развитием и использованием интернета в Республике Беларусь. Доступно через: http://ru.scribd.com/doc/86189304/sokolova.

65. Солдатенко, В. (2012) Правовое регулирование вопросов защиты персональных данных в Республике Беларусь и иностранных государствах. Доступно через: http://pravo.by/Conf2010/reports/Soldatenko.doc.

66. Солоув, Д. (2009) «Мне нечего скрывать» и другие ошибочные толкования приватности. Доступно через: https://www.pgpru.com/biblioteka/statji/nothingtohide.

67. Стецовский, Ю. (2000) Право на свободу и личную неприкосновенность. Нормы и действительность.

68. Суховерхий, В. (1970) Личные неимущественные права граждан в советском гражданском праве.

69. Тарасова, Е. (2013) К вопросу о понятии и защите персональных данных в Республике Беларусь. Доступно через: http://elib.bsu.by/handle/123456789/52196.

70. Фатьянов, А. (1999) Тайна и право (основные системы ограничения в российском праве).

71. Хазиев, Р.(2013) Частная жизнь и ее неприкосновенность как многоаспектный феномен. Доступно через: http://www.eurasialegal.info/index.php?option=com_content&view=article&id=3016:2013-12-11-14-28-36&catid=178:2013-01-18-05-33-28&Itemid=1.

72. Шахов, Н. (2008) Отношения по охране частной жизни и информации о частной жизни как объект теоретико-правового исследования.

73. Шкудунова, Е. (2006) Соотношение публичной и приватной сфер жизнедеятельности.

74. Шрамкова И., Крат Ю. (2008) Защита и обработка конфиденциальных документов.

75. Шугай, А. (2012) Некоторые проблемы защиты персональных данных в Республике Беларусь. Доступно через: http://pravo.by/Conf2012/reports.htm

76. Юрченко И. (2000) Информация конфиденциального характера как предмет уголовно-правовой охраны.

77. Bennett, C. (1992) Regulating Privacy: Data Protection and Public Policy in Europe and the United States.

78. Bennett, C. (1997) 'Understanding Ripple Effects: The Cross–National Adoption of Policy Instruments for Bureaucratic Accountability', Governance, 10 (3), pp. 213–233.

79. Bennett, C. (1998) Application of a Methodology designed to Assess the Adequacy of the Level of Protection of Individuals with regard to Processing Personal Data: Test of the Method on Several Categories of Transfer. European Commission Tender No. XV/97/18/D, September 1998. (Co-authored with Charles D. Raab, Robert M. Gellman and N. Waters). Доступно через: http://www.colinbennett.ca/Recent%20publications/adequat_en.pdf.

80. Bennett, C. (2001) What Government Should Know about Privacy: A Foundation Paper. Доступно через: http://www.colinbennett.ca/wp-content/uploads/2012/06/What-Government-Should-Know-about-Privacy.pdf.

81. Bennett, C. (2008) The Privacy Advocates: Resisting the Spread of Surveillance.

82. Bennett, C. Grant, R. (1999) Visions of Privacy: Policy Choices for the Digital Age.

83. Bennett, C. and Raab, C. (2006) The Governance of Privacy: Policy Instruments in Global Perspective.

84. Bennett, C. (2001) Privacy in the Political System:Perspectives from Political Science and Economics. A report written for the Ethical, Legal and Social Issues (ELSI) component of the Human Genome Project, U.S. Department of Energy. Доступно через: http://www.colinbennett.ca/wp-content/uploads/2012/06/Privacyin-the-Political-System.pdf.

85. Bennett, Colin and Mulligan, Deirdre K. (2012) The Governance of Privacy Through Codes of Conduct: International Lessons for U.S. Privacy Policy. Доступно через: http://ssrn.com/abstract=2230369 orhttp://dx.doi.org/10.2139/ssrn.2230369.

86. Bignami, F. (2005) 'Trans governmental Networks vs. Democracy: The Case of the European Information Privacy Network', Michigan Journal of International Law, 26 (3), pp. 807-868.

87. Bygrave, L. (2002) Data Protection Law: Approaching its Rationale, Logic and Limits.

88. Caplan, J., and J. Torpey, eds. (2001) Documenting individual identity: The development of state practices in the modern world.

89. Carlsson, I. et al. UN, Commission on Global Governance. (1995). Our global neighborhood.

90. Clarke, R. (1987) Another Piece of Plastic for Your Wallet: The Australia Card Scheme. Доступно через: http://www.anu.edu.au/people/Roger.Clarke/DV/OzCard.html.

91. Clarke, R. (1988) 'Information Technology and Dataveillance. Communications of the ACM 31, no. 5 P. 498-512.

92. Craig, T., Ludoff, M. (2011) Privacy and Big Data: The Players, Regulators, and Stakeholders.

93. Curry, M. (2002) Everyday practices in public spaces. Доступно через: http://baja.sscnet.ucla.edu/~curry/Curry--Everyday_practices.pdf.

94. Dandeker, Ch. (1990) Surveillance, Power, and Modernity: Bureaucracy and Discipline from 1700 to the Present Day.

95. Data Protection, Human Rights and Democratic Values: XIII Conference of the Data Protection Commissioners 2-4 October 1991. Доступно через: http://phdtree.org/pdf/26705946-xiiith-conference-of-data-protection-commissioners-strasbourg-24-october-1991/.

96. Drinan, R. (2001) The Mobilization of Shame: A World View of Human Rights. New Haven:Yale University Press.

97. Emerson, Th. (1989) The Right for Privacy and Freedom of Press. Доступно через: http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=3789&context=fss_papers.

98. Etzioni, A. (1999) The Limits Of Privacy. Доступно через: http://www.questia.com/library/1393933/the-limits-of-privacy#/.

99. Federal Trade Commission (1998) Privacy online: a report to Congress. Доступно через: http://www.ftc.gov/reports/privacy3/toc.shtm.

100. Ferraris, V et al (2013) Defining Profiling. Доступно через: http://profiling-project.eu/wp-content/uploads/2013/07/PROFILINGproject_WS1_definition_2607.pdf.

101. Flaherty, D. (1989) Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States.

102. Franclin, E.H. (1996) Business guide to Privacy and Data Protection Legislation.

103. Galexia (2008) The US Safe Harbor – Fact or Fiction? Доступно через: http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safeharbor_fact_or_fiction-Introduc.html.

104. Gellman, R. (2014) Fair Information Practices: A Basic History. Доступно через: http://www.bobgellman.com/rg-docs/rg-FIPShistory.pdf.

105. Gartner Special Repot (2012) Pattern-Based Strategy: Getting Value from Big Data "Pattern-Based Strategy: Getting Value from Big Data".

106. Greenleaf, G. (2011) Global Data Privacy in a Networked World. Доступно через: http://ssrn.com/abstract=1954296.

107. Hert, P. (2013) Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency? Доступно через: http://moritzlaw.osu.edu/students/groups/is/files/2013/08/7-Hert-Papakonstantinou.pdf.

108. ICC Task Force on Privacy and Protection of Personal Data (2004) ICC report on binding corporate rules for international transfers of personal data. Доступно через: http://www.iccwbo.org/Data/Documents/Digital-Economy/ICC-report-on-Binding-Corporate-Rules/.

109. ICC (2003) Privacy Toolkit. An international business guide for policymakers. Доступно через: http://www.iccwbo.org/privacy_toolkit/.

110. Kirby, M. (1999) Privacy Protection – A New Beginning, (speech before the 21st International Conference on Privacy and Personal Data Protection. Доступно через: http://www.pco.org.hk/english/infocentre/conference.html.

111. Lessig, L. (1999b) Code and Other Laws of Cyberspace.

112. Loring T (2002) An analysis of the informational privacy protection afforded by the European Union and the United States. Доступно через: http://www.highbeam.com/doc/1P3-114483467.html.

113. Lyon, D. (1994) The Electronic Eye: The Rise of Surveillance Society.

114. Lyon, D. (2001) Surveillance Society: Monitoring Everyday Life.

115. Lyon, D. (2003) Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination.

116. Lyon, D. (2003) Surveillance after September 11th. Cambridge: Polity Press.

117. Lyon, D. (2007) Surveillance Studies: An Overview.

118. Moore,B. (1984) Privacy: Studies in Social and Cultural History.

119. Nissenbaum, H. (2004) Privacy as Contextual Integrity. Доступно через: http://ssrn.com/abstract=534622.

120. Post, R. (2001) Three Concepts of Privacy. Доступно через: http://digitalcommons.law.yale.edu/fss_papers/185.

121. Norris, C., and G. Armstrong. 1999: The maximum surveillance society: the rise of CCTV.

122. Parent, W. A. (1983) Privacy, Morality, and the Law. Philosophy and Public Affairs, vol-12, no. 4 Princeton University Press, pp. 269-88.

123. Pierre, J. (2000) Debating Governance: Authority, Steering, and Democracy. Доступно через: http://www.research.ed.ac.uk/portal/files/12592176/Privacy_Actors_Performances_and_the_Future_of_Privacy_Protection.pdf.

124. Penney, J. (2008) Privacy and the new virtualism. Доступно через: http://digitalcommons.law.yale.edu/yjolt/vol10/iss1/6.

125. Peters, A. (Ed.). (2009). Non-state actors as standard setters. Cambridge: Cambridge University Press.

126. Post, R. (1989) The Social Foundations of privacy. Доступно через: http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1210&context=fss_papers.

127. Post, R. (1991) Rereading Warren and Brandeis: Privacy, Property, and Appropriation. Доступно через: http://digitalcommons.law.yale.edu/fss_papers/206.

128. Pierre, J. (2000) Debating Governance: Authority, Steering, and Democracy.

129. Prosser, W. (1960) Privacy [A legal analysis].

130. Raab, C, Koops, B-J (2009), Privacy Actors, Performances and the Future of Privacy Protection. Доступно через: http://www.research.ed.ac.uk/portal/files/12592176/Privacy_Actors_Performances_and_the_Future_of_Privacy_Protection.pdf.

131. Raab, C. (2010), Information Privacy: Networks of Regulation at the Subglobal Level. Global Policy, 1: 291-302.

132. Raab, C., Hert, P. (2007) The regulation of Technology: Policy Tools and Policy Actors. Доступно через: http://tilburguniversity.nl/tilt/publications/workingpapers.

133. Raab, C. (2014) Privacy as Security Value. Доступно через: http://bigdataandprivacy.org/wp-content/uploads/2014/08/Raab_PrivacySecurityValue.pdf.

134. Raab, C. Privacy Protection: Revisiting Four Concepts. Доступно через: http://alexandrie.droit.fundp.ac.be/GEIDEFile/6945.pdf?Archive=193021391120&File=6945_pdf.

135. Raab, Charles D. Beyond Activism: Research Perspectives on Privacy. Доступно через: http://ssrn.com/abstract=1096562 or http://dx.doi.org/10.2139/ssrn.1096562.

136. Raab, Charles D. and Goold, Benjamin J. (2011) Protecting Information. Доступно через: http://ssrn.com/abstract=1967198.

137. Rosenau, J. (1990). Turbulence in world politics: a theory of change and continuity.

138. Regan, P. (1995) Legislating Privacy: Technology, Social Values and Public Policy.

139. Richards, Neil M. (2009) Privacy and the Limits of History. Доступно через: http://digitalcommons.law.yale.edu/yjlh/vol21/iss1/4.

140. Rule, J. et al. (1980) The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies.

141. Rubenfeld, J. (2008) The End of Privacy. Доступно через: http://digitalcommons.law.yale.edu/fss_papers/1552.

142. Rubenfeld, J. (1989) The Right of Privacy. Доступно через: http://digitalcommons.law.yale.edu/fss_papers/156.

143. Sadilek, A., Krumm, J. (2012) Far Out: Predicting Long-Term Human Mobility. Доступно через: http://www.cs.rochester.edu/~sadilek/publications/Sadilek-Krumm_Far-Out_AAAI-12.pdf.

144. Schoeman, F. (1992) Privacy and Social Freedom. Доступно через: doi: 10.1111/j.1758-5899.2010.00030.x.

145. Scoglio, S. (1998) Transforming Privacy: A Transpersonal Philosophy of Rights.

146. Schwartz, P. (1999) ‘Privacy and Democracy in Cyberspace. Vanderbilt Law Review 52, no. 6. PP 1610–1702.

147. Sieghart, P. (1976) Privacy and Computers.

148. Steeves, V. Reclaiming the Social Value of Privacy. Доступно через: http://www.idtrail.org/files/ID%20Trail%20Book/9780195372472_kerr_11.pdf.

149. Tan, J. (2008) A comparative study of the APEC privacy framework: A new voice in the data protection dialogue? Доступно черезhttp://www.degruyter.com/dg/viewarticle/j$002fasjcl.2008.3.1$002fasjcl.2008.3.1.1071$002fasjcl.2008.3.1.1071.xml;jsessionid=F36717919BBF04391AC61CF44A516545.

150. Taipale, K. (2005) Technology, security and privacy: the fear of Frankenstein, the mythology of privacy and the lessons of king Ludd. Доступно через: http://digitalcommons.law.yale.edu/yjolt/vol7/iss1/6.

151. Tucker, P. (2013) Has Big Data Made Anonymity Impossible? Доступно через: http://www.technologyreview.com/news/514351/has-big-data-made-anonymity-impossible.

152. Wakes, R. (1980) Protection of Privacy.

153. Westin, A. (1967) Privacy and Freedom.

154. Westin, A. Baker, M. (1972) Databanks in a Free Society: Computers, Record-Keeping and Privacy.

155. Westin, A. (2003) Social and Political Dimensions of Privacy. Доступно через V.59 http://www.asc.upenn.edu/usr/ogandy/Gandy%20Comm664/westin%20-%20social%20and%20political%20dimensions%20of%20privacy.pdf.

156. Whitman, J. (2004) The Two Western Cultures of Privacy: Dignity versus Liberty. Достъпно чрез: http://digitalcommons.law.yale.edu/fss_papers/649.

157. Wugmeister, M. (2011) Privacy law: International data protection developments. Twelfth Annual Institute on Privacy and Data Security Law .

УЧЕБНОЕ ПОСОБИЕ

А. Пазюк, М. Соколова

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ:
ВВЕДЕНИЕ В ПРОБЛЕМАТИКУ

Корректор В. Синюхин
Оформление, верстка Bazinato

Формат А4
Бумага офсетная.
Печать офсетная
Тираж 300 экз.

BSPB, UAB
Kauno g. 36-230,
LT-03202
Vilnius